

# HP A3100 v2 Switch Series

## Fundamentals

### Configuration Guide

HP A3100-8 v2 SI Switch (JG221A)

HP A3100-16 v2 SI Switch (JG222A)

HP A3100-24 v2 SI Switch (JG223A)

HP A3100-8 v2 EI Switch (JD318B)

HP A3100-16 v2 EI Switch (JD319B)

HP A3100-24 v2 EI Switch (JD320B)

HP A3100-8-PoE v2 EI Switch (JD311B)

HP A3100-16-PoE v2 EI Switch (JD312B)

HP A3100-24-PoE v2 EI Switch (JD313B)

Part number: 5998-1963

Software version: Release 5103

Document version: 6W100-20110909



**Legal and notice information**

© Copyright 2011 Hewlett-Packard Development Company, L.P.

No part of this documentation may be reproduced or transmitted in any form or by any means without prior written consent of Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

---

# Contents

CLI configuration .....	1
What is CLI? .....	1
Entering the CLI .....	1
Command conventions .....	1
Undo form of a command .....	2
CLI view description .....	2
Entering system view .....	3
Exiting the current view .....	3
Returning to user view .....	4
Using the CLI online help .....	4
Typing commands .....	5
Editing command lines .....	5
Typing incomplete keywords .....	5
Configuring command aliases .....	6
Configuring CLI hotkeys .....	6
Redisplaying input but not submitted commands .....	8
Checking command-line errors .....	8
Using command history .....	8
Accessing history commands .....	9
Configuring the history buffer size .....	9
Controlling the CLI display .....	10
Multi-screen display .....	10
Filtering output information .....	10
Configuring user privilege and command levels .....	13
Introduction .....	13
Configuring a user privilege level .....	14
Switching user privilege level .....	16
Modifying the level of a command .....	19
Saving the current configuration .....	20
Displaying and maintaining CLI .....	20
Login methods .....	21
Login methods .....	21
User interface overview .....	22
Users and user interfaces .....	22
Numbering user interfaces .....	22
CLI login .....	24
Overview .....	24
Logging in through the console port .....	24
Introduction .....	24
Configuration requirements .....	24
Login procedure .....	25
Console login authentication modes .....	27
Configuring none authentication for console login .....	28
Configuring password authentication for console login .....	29
Configuring scheme authentication for console login .....	31
Configuring common settings for console login (optional) .....	34
Logging in through Telnet .....	36
Introduction .....	36

Telnet login authentication modes .....	37
Configuring none authentication for Telnet login .....	38
Configuring password authentication for Telnet login .....	39
Configuring scheme authentication for Telnet login .....	41
Configuring common settings for VTY user interfaces (optional).....	45
Configuring the device to log in to a Telnet server as a Telnet client.....	46
Logging in through SSH .....	47
Introduction .....	47
Configuring the SSH server.....	48
Configuring the SSH client to log in to the SSH server .....	51
Logging in through modems .....	52
Introduction .....	52
Configuration requirements.....	52
Login procedure.....	52
Modem login authentication modes.....	55
Configuring none authentication for modem login.....	56
Configuring password authentication for modem login.....	57
Configuring scheme authentication for modem login .....	58
Configuring common settings for modem login (optional).....	62
Displaying and maintaining CLI login .....	64
<b>Web login .....</b>	<b>66</b>
Web login overview .....	66
Configuring HTTP login .....	66
Configuring HTTPS login .....	67
Displaying and maintaining web login .....	70
Web login example.....	70
HTTP login example .....	70
HTTPS login example .....	71
<b>NMS login .....</b>	<b>74</b>
NMS login overview.....	74
Configuring NMS login.....	74
NMS login example.....	75
<b>User login control.....</b>	<b>78</b>
User login control methods .....	78
Configuring login control over Telnet users.....	78
Configuration preparation.....	78
Configuring source IP-based login control over Telnet users .....	78
Configuring source and destination IP-based login control over Telnet users .....	79
Configuring source MAC-based login control over Telnet users .....	79
Source MAC-based login control configuration example.....	80
Configuring source IP-based login control over NMS users.....	81
Configuration preparation.....	81
Configuring source IP-based login control over NMS users .....	81
Source IP-based login control over NMS users configuration example .....	82
Configuring source IP-based login control over web users .....	83
Configuration preparation.....	83
Configuring source IP-based login control over web users.....	83
Logging off online web users .....	83
Source IP-based login control over web users configuration example .....	84
<b>FTP configuration.....</b>	<b>85</b>
FTP overview.....	85
Introduction to FTP .....	85

FTP operation .....	85
Configuring the FTP client .....	86
Establishing an FTP connection .....	86
Operating the directories on an FTP server .....	87
Operating the files on an FTP server .....	88
Using another username to log in to an FTP server .....	89
Maintaining and debugging an FTP connection .....	89
Terminating an FTP connection .....	89
FTP client configuration example .....	90
Configuring the FTP server .....	91
Configuring FTP server operating parameters .....	91
Configuring authentication and authorization on the FTP server .....	92
FTP server configuration example .....	93
Displaying and maintaining FTP .....	95
<b>TFTP configuration .....</b>	<b>96</b>
TFTP overview .....	96
Introduction to TFTP .....	96
TFTP operation .....	96
Configuring the TFTP client .....	97
Displaying and maintaining the TFTP client .....	98
TFTP client configuration example .....	98
<b>File management .....</b>	<b>100</b>
Managing files .....	100
Filename formats .....	100
Performing directory operations .....	100
Displaying directory information .....	101
Displaying the current working directory .....	101
Changing the current working directory .....	101
Creating a directory .....	101
Removing a directory .....	101
Performing file operations .....	101
Displaying file information .....	102
Displaying the contents of a file .....	102
Renaming a file .....	102
Copying a file .....	102
Moving a file .....	102
Deleting a file .....	102
Restoring a file from the recycle bin .....	103
Emptying the recycle bin .....	103
Performing batch operations .....	103
Performing storage medium operations .....	104
Managing the space of a storage medium .....	104
Setting prompt modes .....	104
Example for file operations .....	104
<b>Configuration file management .....</b>	<b>106</b>
Configuration file overview .....	106
Types of configuration .....	106
Format and content of a configuration file .....	106
Coexistence of multiple configuration files .....	107
Startup with the configuration file .....	107
Saving the running configuration .....	107
Introduction .....	107
Modes in saving the configuration .....	107

Setting configuration rollback .....	108
Configuration rollback .....	108
Configuration task list .....	109
Configuring parameters for saving the running configuration .....	109
Enabling automatic saving of the running configuration .....	110
Manually saving the running configuration .....	110
Setting configuration rollback .....	111
Specifying a startup configuration file to be used at the next system startup .....	111
Backing up the startup configuration file .....	112
Deleting a startup configuration file .....	112
Restoring a startup configuration file .....	113
Displaying and maintaining a configuration file .....	113
<b>Software upgrade configuration .....</b>	<b>115</b>
Switch software overview .....	115
Software upgrade methods .....	115
Upgrading the Boot ROM program through a system reboot .....	116
Upgrading system software through a system reboot .....	117
Software upgrade by installing hotfixes .....	117
Basic concepts in hotfix .....	117
Patch status .....	118
Configuration prerequisites .....	120
One-step patch installation .....	121
Step-by-step patch installation .....	121
Step-by-step patch uninstallation .....	122
Displaying and maintaining the software upgrade .....	123
Software upgrade configuration examples .....	123
Scheduled upgrade configuration example .....	123
Hotfix configuration example .....	125
<b>Device management .....</b>	<b>126</b>
Configuring the device name .....	126
Changing the system time .....	126
Configuration guidelines .....	126
Configuration procedure .....	129
Enabling displaying the copyright statement .....	129
Configuring banners .....	130
Introduction to banners .....	130
Configuration procedure .....	131
Banner configuration examples .....	131
Configuring the exception handling method .....	131
Rebooting the device .....	132
Rebooting the device immediately at the CLI .....	132
Scheduling a device reboot .....	132
Scheduling jobs .....	133
Job configuration approaches .....	133
Configuration guidelines .....	133
Scheduling a job in the non-modular approach .....	134
Scheduling a job in the modular approach .....	134
Disabling Boot ROM access .....	134
Configuring the detection timer .....	135
Configuring temperature alarm thresholds (available only on the A3100 v2 EI) .....	135
Clearing idle 16-bit interface indexes .....	136
Verifying and diagnosing transceiver modules .....	136
Verifying transceiver modules .....	136

Diagnosing transceiver modules.....	137
Displaying and maintaining device management configuration .....	137
<b>Automatic configuration .....</b>	<b>140</b>
Automatic configuration overview.....	140
Typical automatic configuration network.....	140
How automatic configuration works .....	141
Work flow of automatic configuration .....	141
Using DHCP to obtain an IP address and other configuration information .....	142
Obtaining the configuration file from the TFTP server .....	143
Executing the configuration file.....	145
<b>Support and other resources .....</b>	<b>146</b>
Contacting HP .....	146
Subscription service .....	146
Related information .....	146
Documents.....	146
Websites.....	146
Conventions .....	147
<b>Index .....</b>	<b>149</b>

---

# CLI configuration

## What is CLI?

The command line interface (CLI) enables you to interact with your device by typing text commands. At the CLI, you can instruct your device to perform a given task by typing a text command and then pressing **Enter**. Compared with a graphical user interface (GUI) where you can use a mouse to perform configuration, the CLI allows you to input more information in one command line.

**Figure 1 CLI example**

```
User interface aux0 is available.

Press ENTER to get started.
<HP>system-view
System View: return to User View with Ctrl+Z.
[HP]
```

## Entering the CLI

HP devices provide multiple methods for entering the CLI, such as through the console port, through Telnet, or through SSH. For more information, see the chapter “Logging in to the switch configuration.”

## Command conventions

Command conventions help you understand command meanings. Commands in HP product manuals comply with the conventions listed in [Table 1](#).

**Table 1 Command conventions**

Convention	Description
<b>Boldface</b>	<b>Bold</b> text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	<i>Italic</i> text represents arguments that you replace with actual values.



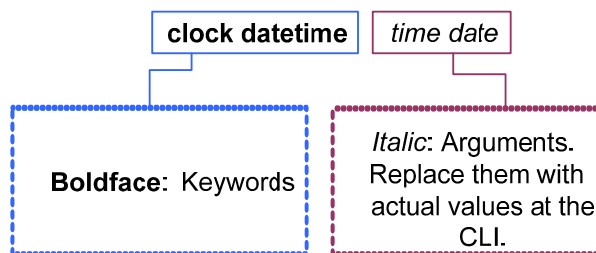
Convention	Description
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x   y   ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[ x   y   ... ]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x   y   ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[ x   y   ... ] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

**NOTE:**

The keywords of HP command lines are case insensitive.

Figure 2 shows how to read the **clock datetime** *time date* command by using Table 1 as a reference.

**Figure 2 Read command line parameters**



Following this example, you can type the following command line at the CLI of your device and press **Enter** to set the device system time to 10 o'clock 30 minutes 20 seconds, February 23, 2010.

```
<sysname> clock datetime 10:30:20 2/23/2010
```

More complicated commands can be understood using Table 1 as a reference.

## Undo form of a command

The **undo** form of a command restores the default, disables a function, or removes a configuration.

Almost all configuration commands have an **undo** form. For example, the **info-center enable** command enables the information center, and the **undo info-center enable** command disables the information center.

## CLI view description

Commands are grouped into different classes by function. To use a command, you must enter the class view of the command.

CLI views adopt a hierarchical structure. See [Figure 3](#).

- After logging in to the switch, you are in user view. The user view prompt is `<device name>`. In user view, you can perform display, debugging, and file management operations, set the system time, restart your device, and perform FTP and Telnet operations.
- You can enter system view from user view. In system view, you can configure parameters such as daylight saving time, banners, and short-cut keys.
- From system view, you can enter different function views. For example, enter interface view to configure interface parameters, create a VLAN and enter its view, enter user interface view to configure login user attributes, create a local user and enter local user view to configure the password and level of the local user.

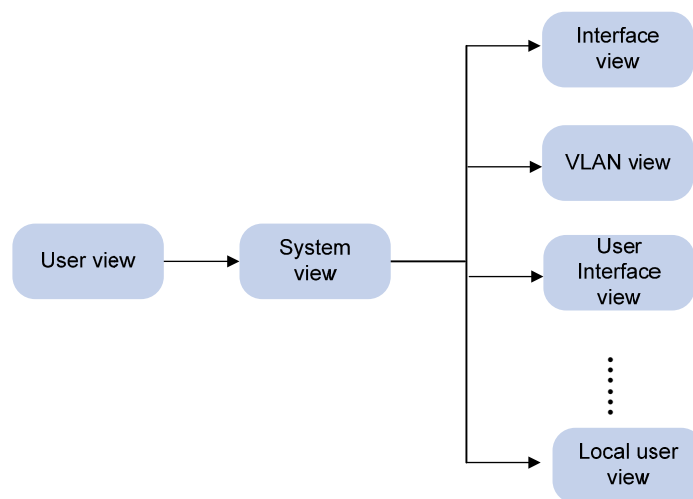
---

**NOTE:**

Enter `?` in any view to display all the commands that can be executed in this view.

---

**Figure 3 Command line views**



## Entering system view

When you log in to the device, you automatically enter user view, where `<Device name>` is displayed. You can perform limited operations in user view, for example, display operations, file operations, and Telnet operations. To perform further configuration on the device, enter system view.

Follow the step below to enter system view:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	Required Available in user view

## Exiting the current view

The CLI is divided into different command views. Each view has a set of specific commands and defines the effective scope of the commands. The commands available to you at any given time depend on the view you are in.

Follow the step below to exit the current view:

To do...	Use the command...	Remarks
Return to the parent view from the current view	<b>quit</b>	Required Available in any view.

**NOTE:**

- The **quit** command in user view stops the current connection between the terminal and the device.
- In public key code view, use the **public-key-code end** command to return to the parent view (public key view). In public key view, use the **peer-public-key end** command to return to system view.

## Returning to user view

This feature allows you to return to user view from any other view, without using the **quit** command repeatedly. You can also press **Ctrl+Z** to return to user view from the current view.

Follow the step below to exit to user view:

To do...	Use the command...	Remarks
Return to user view	<b>return</b>	Required Available in any view except user view

## Using the CLI online help

Type a question mark (?) to obtain online help. See the following examples.

1. Type **?** in any view to display all commands available in this view as well as brief descriptions of the commands. For example:

```
<sysname> ?
```

```
User view commands:
```

```
archive          Specify archive settings
backup           Backup next startup-configuration file to TFTP server
boot-loader      Set boot loader
bootrom          Update/read/backup/restore bootrom
cd               Change current directory
```

```
...Omitted...
```

2. Type part of a command and a **?** separated by a space.

If **?** is at the keyword position, the CLI displays all possible keywords with a brief description for each keyword. For example:

```
<sysname> terminal ?
```

```
debugging      Send debug information to terminal
logging        Send log information to terminal
monitor        Send information output to current terminal
trapping       Send trap information to terminal
```

If **?** is at the argument position, the CLI displays a description about this argument. For example:

```
<sysname> system-view
```

```
[sysname] interface vlan-interface ?
```

```

<1-4094> VLAN interface
[sysname] interface vlan-interface 1 ?
<cr>
[sysname] interface vlan-interface 1

```

The string **<cr>** indicates that the command is a complete command, and can be executed by pressing **Enter**.

3. Type an incomplete character string followed by **?**. The CLI displays all commands starting with the typed character(s).

```

<sysname> b?
  backup
  boot-loader
  bootrom
<sysname> display cl?
  clipboard
  clock
  cluster

```

## Typing commands

### Editing command lines

**Table 2** Editing functions

Key	Function
Common keys	If the edit buffer is not full, pressing a common key inserts the character at the position of the cursor and moves the cursor to the right.
<b>Backspace</b>	Deletes the character to the left of the cursor and moves the cursor back one character.
Left arrow key or <b>Ctrl+B</b>	The cursor moves one character space to the left.
Right arrow key or <b>Ctrl+F</b>	The cursor moves one character space to the right.
<b>Tab</b>	<p>If you press <b>Tab</b> after entering part of a keyword, the system automatically completes the keyword:</p> <ul style="list-style-type: none"> <li>• If there is a unique match, the system substitutes the complete keyword for the incomplete one and displays it in the next line.</li> <li>• If there is more than one match, you can press <b>Tab</b> repeatedly to cycle through all the keywords starting with the character string that you typed.</li> <li>• If there is no match, the system does not modify the incomplete keyword and displays it again in the next line.</li> </ul>

### Typing incomplete keywords

You can input a command comprising incomplete keywords that uniquely identify the complete command.

In user view, for example, commands starting with an **s** include **startup saved-configuration** and **system-view**.

- To enter system view, type **sy**.

- To set the configuration file for next startup, type **st s**.

You can also press **Tab** to have an incomplete keyword automatically completed.

## Configuring command aliases

The command alias function allows you to replace the first keyword of a command with your preferred keyword. For example, if you configure **show** as the replacement for the **display** keyword, then to execute the **display xx** command, you can input the command alias **show xx**.

Note the following guidelines when configuring a command alias:

- You can define and use a command alias but the command is not restored in its alias format.
- When you define a command alias, the *cmdkey* and *alias* arguments must be in their complete form.
- When you input an incomplete keyword that partially matches both a defined alias and the keyword of a command, the alias takes precedence. To execute the command whose keyword partially matches your input, input the complete keyword. When you input a character string that partially matches multiple aliases, the system gives you prompts.
- If you press **Tab** after you input an alias keyword, the original format of the keyword is displayed.
- You can replace only the first keyword of a non-undo command instead of the complete command. You can replace only the second keyword of **undo** commands.

Follow these steps to configure command aliases:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enable the command alias function	<b>command-alias enable</b>	Required Disabled by default, which means you cannot configure command aliases.
Configure a command alias	<b>command-alias mapping</b> <i>cmdkey</i> <i>alias</i>	Required Not configured by default.

## Configuring CLI hotkeys

Follow these steps to configure CLI hotkeys:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Configure CLI hotkeys	<b>hotkey</b> { <b>CTRL_G</b>   <b>CTRL_L</b>   <b>CTRL_O</b>   <b>CTRL_T</b>   <b>CTRL_U</b> } <i>command</i>	Optional The <b>Ctrl+G</b> , <b>Ctrl+L</b> and <b>Ctrl+O</b> hotkeys are specified at the CLI by default.
Display hotkeys	<b>display hotkey</b>	Available in any view. See <a href="#">Table 3</a> for hotkeys reserved by the system.

---

**NOTE:**

By default, the **Ctrl+G**, **Ctrl+L** and **Ctrl+O** hotkeys are associated with pre-defined commands as defined below, the **Ctrl+T** and **Ctrl+U** hotkeys are not.

- **Ctrl+G** corresponds to the **display current-configuration** command.
  - **Ctrl+L** corresponds to the **display ip routing-table** command.
  - **Ctrl+O** corresponds to the **undo debugging all** command.
- 

**Table 3 Hotkeys reserved by the system**

Hotkey	Function
<b>Ctrl+A</b>	Moves the cursor to the beginning of the current line.
<b>Ctrl+B</b>	Moves the cursor one character to the left.
<b>Ctrl+C</b>	Stops performing a command.
<b>Ctrl+D</b>	Deletes the character at the current cursor position.
<b>Ctrl+E</b>	Moves the cursor to the end of the current line.
<b>Ctrl+F</b>	Moves the cursor one character to the right.
<b>Ctrl+H</b>	Deletes the character to the left of the cursor.
<b>Ctrl+K</b>	Terminates an outgoing connection.
<b>Ctrl+N</b>	Displays the next command in the history command buffer.
<b>Ctrl+P</b>	Displays the previous command in the history command buffer.
<b>Ctrl+R</b>	Redisplays the current line information.
<b>Ctrl+V</b>	Pastes the content in the clipboard.
<b>Ctrl+W</b>	Deletes all the characters in a continuous string to the left of the cursor.
<b>Ctrl+X</b>	Deletes all characters to the left of the cursor.
<b>Ctrl+Y</b>	Deletes all characters to the right of the cursor.
<b>Ctrl+Z</b>	Exits to user view.
<b>Ctrl+]</b>	Terminates an incoming connection or a redirect connection.
<b>Esc+B</b>	Moves the cursor to the leading character of the continuous string to the left.
<b>Esc+D</b>	Deletes all the characters of the continuous string at the current cursor position and to the right of the cursor.
<b>Esc+F</b>	Moves the cursor to the front of the next continuous string to the right.
<b>Esc+N</b>	Moves the cursor down by one line (available before you press <b>Enter</b> )
<b>Esc+P</b>	Moves the cursor up by one line (available before you press <b>Enter</b> )
<b>Esc+&lt;</b>	Specifies the cursor as the beginning of the clipboard.
<b>Esc+&gt;</b>	Specifies the cursor as the ending of the clipboard.

---

---

**NOTE:**

The hotkeys in [Table 3](#) are defined by the switch. If the same hotkeys are defined by the terminal software that you use to interact with the switch, the hotkeys defined by the terminal software take effect.

---

## Redisplaying input but not submitted commands

If your command input is interrupted by output system information, you can use this feature to redisplay the commands input previously but not submitted.

Follow these steps to enable redisplaying of commands previously input but not submitted:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enable redisplaying of input but not submitted commands	<b>info-center synchronous</b>	Required Disabled by default

---

**NOTE:**

- If you have no input at the command line prompt and the system outputs system information such as logs, the system will not display the command line prompt after the output.
  - If the system outputs system information when you are typing interactive information (not YES/NO for confirmation), the system does not redisplay the prompt information but a line break after the output and then display what you have typed.
  - For more information about the **info-center synchronous** command, see the *Network Management and Monitoring Configuration Guide*.
- 

## Checking command-line errors

If a command contains syntax errors, the CLI reports error information.

**Table 4 Common command line errors**

Error information	Cause
% Unrecognized command found at '^' position.	The command was not found.
% Incomplete command found at '^' position.	Incomplete command
% Ambiguous command found at '^' position.	Ambiguous command
Too many parameters	Too many parameters
% Wrong parameter found at '^' position.	Wrong parameters

---

## Using command history

The CLI automatically saves the commands recently used in the history command buffer. You can access these commands and execute them again.

## Accessing history commands

Follow a step below to access history commands:

To do...	Use the key/command...	Result
Display history commands	<b>display history-command</b>	Displays valid history commands you used
Display the previous history command	Up arrow key or <b>Ctrl+P</b>	Displays the previous history command, if any
Display the next history command	Down arrow key or <b>Ctrl+N</b>	Displays the next history command, if any

### NOTE:

You can use arrow keys to access history commands in Windows 200X and XP Terminal or Telnet. However, the up and down arrow keys are invalid in Windows 9X HyperTerminal, because they are defined differently. You can use **Ctrl+P** or **Ctrl+N** instead.

- The commands saved in the history command buffer are in the same format in which you typed the commands. If you type an incomplete command, the command saved in the history command buffer is also incomplete.
- If you execute the same command repeatedly, the switch saves only the earliest record. However, if you execute the same command in different formats, the system saves them as different commands. For example, if you execute the **display cu** command repeatedly, the system saves only one command in the history command buffer. If you execute the command in the format of **display cu** and **display current-configuration** respectively, the system saves them as two separate commands.
- By default, the CLI can save up to 10 commands for each user. To set the capacity of the history command buffer for the current user interface, use the **history-command max-size** command. (For more information about the **history-command max-size** command, see the chapter “Logging in to the switch commands.”)

## Configuring the history buffer size

Follow these steps to configure the history buffer size:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enter user interface view	<b>user-interface</b> { <i>first-num1</i> [ <i>last-num1</i> ]   { <b>aux</b>   <b>vty</b> } <i>first-num2</i> [ <i>last-num2</i> ] }	—
Set the maximum number of commands that can be saved in the history buffer	<b>history-command max-size</b> <i>size-value</i>	Optional By default, the history buffer can save up to 10 commands.

### NOTE:

For more information about the **user-interface** and **history-command max-size** commands, see the chapter “Logging in to the switch commands.”



# Controlling the CLI display

## Multi-screen display

### Controlling multi-screen display

If the output information spans multiple screens, each screen pauses after it is displayed. Perform one of the following operations to proceed.

Action	Function
Press <b>Space</b>	Displays the next screen.
Press <b>Enter</b>	Displays the next line.
Press <b>Ctrl+C</b>	Stops the display and the command execution.
Press <b>&lt;PageUp&gt;</b>	Displays the previous page.
Press <b>&lt;PageDown&gt;</b>	Displays the next page.

By default, each screen displays up to 24 lines. To change the maximum number of lines displayed on the next screen, use the **screen-length** command. For more information about the **screen-length** command, see the chapter “Logging in to the switch commands.”

### Disabling multi-screen display

You can use the following command to disable the multi-screen display function. All of the output information will be displayed at one time and the screen will refresh continuously until the last screen is displayed.

To do...	Use the command...	Remarks
Disable the multi-screen display function	<b>screen-length disable</b>	<p>Required</p> <p>By default, a login user uses the settings of the <b>screen-length</b> command. The default settings of the <b>screen-length</b> command are: multiple-screen display is enabled and up to 24 lines are displayed on the next screen.</p> <p>This command is executed in user view, and takes effect for the current user only. When the user re-logs into the switch, the default configuration is restored.</p>

## Filtering output information

### Introduction

You can use regular expressions in **display** commands to filter output information.

The following methods are available for filtering output information:

- Input the **begin**, **exclude**, or **include** keyword plus a regular expression in the **display** command to filter the output information.

- When the system displays the output information in multiple screens, use /, - or + plus a regular expression to filter subsequent output information. / equals the keyword **begin**, - equals the keyword **exclude**, and + equals the keyword **include**.

The following definitions apply to the **begin**, **exclude**, and **include** keywords:

- **begin**: Displays the first line that matches the specified regular expression and all lines that follow.
- **exclude**: Displays all lines that do not match the specified regular expression.
- **include**: Displays all lines that match the specified regular expression.

A regular expression is a case-sensitive string of 1 to 256 characters. It supports the following special characters.

Character	Meaning	Remarks
^string	Starting sign. <i>string</i> appears only at the beginning of a line.	For example, regular expression " <b>^user</b> " only matches a string beginning with "user", not "Auser".
string\$	Ending sign. <i>string</i> appears only at the end of a line.	For example, regular expression "user <b>\$</b> " only matches a string ending with "user", not "userA".
.	Matches any single character, such as a single character, a special character, and a blank.	For example, ".s" matches "as" and "bs".
*	Matches the preceding character or character group zero or multiple times.	For example, "zo*" matches "z" and "zoo"; "(zo)*" matches "zo" and "zozo".
+	Matches the preceding character or character group one or multiple times	For example, "zo+" matches "zo" and "zoo", but not "z".
	Matches the preceding or succeeding character string	For example, "def int" only matches a character string containing "def" or "int".
_	If it is at the beginning or the end of a regular expression, it equals ^ or \$. In other cases, it equals comma, space, round bracket, or curly bracket.	For example, "a_b" matches "a b" or "a(b"; "_ab" only matches a line starting with "ab"; "ab_" only matches a line ending with "ab".
-	Connects two values (the smaller one before it and the bigger one after it) to indicate a range together with [ ].	For example, "1-9" means 1 to 9 (inclusive); "a-h" means a to h (inclusive).
[ ]	Matches a single character contained within the brackets.	For example, [16A] matches a string containing any character among 1, 6, and A; [1-36A] matches a string containing any character among 1, 2, 3, 6, and A (- is a hyphen). "]" can be matched as a common character only when it is put at the beginning of characters within the brackets, for example [ ]string]. There is no such limit on "[".
( )	A character group. It is usually used with "+" or "*".	For example, (123A) means a character group "123A"; "408(12)+" matches 40812 or 408121212. But it does not match 408.

Character	Meaning	Remarks
<code>\index</code>	Repeats the character string specified by the index. A character string refers to the string within () before <code>\</code> . <code>index</code> refers to the sequence number (starting from 1 from left to right) of the character group before <code>\</code> . If only one character group appears before <code>\</code> , <code>index</code> can only be 1; if <code>n</code> character groups appear before <code>index</code> , <code>index</code> can be any integer from 1 to <code>n</code> .	For example, <code>(string)\1</code> repeats <code>string</code> , and a matching string must contain <code>stringstring</code> . <code>(string1)(string2)\2</code> repeats <code>string2</code> , and a matching string must contain <code>string1string2string2</code> . <code>(string1)(string2)\1\2</code> repeats <code>string1</code> and <code>string2</code> respectively, and a matching string must contain <code>string1string2string1string2</code> .
<code>[^]</code>	Matches a single character not contained within the brackets.	For example, <code>[^16A]</code> means to match a string containing any character except 1, 6 or A, and the matching string can also contain 1, 6 or A, but cannot contain these three characters only. For example, <code>[^16A]</code> matches "abc" and "m16", but not 1, 16, or 16A.
<code>\&lt;string</code>	Matches a character string starting with <code>string</code> .	For example, <code>"\&lt;do"</code> matches word "domain" and string "doa".
<code>string\&gt;</code>	Matches a character string ending with <code>string</code> .	For example, <code>"do\&gt;"</code> matches word "undo" and string "abcdo".
<code>\bcharacter2</code>	Matches <code>character1character2</code> . <code>character1</code> can be any character except number, letter or underline, and <code>\b</code> equals <code>[^A-Za-z0-9_]</code> .	For example, <code>"\ba"</code> matches "a" with "-" being <code>character1</code> , and "a" being <code>character2</code> , but it does not match "2a" or "ba".
<code>\Bcharacter</code>	Matches a string containing <code>character</code> , and no space is allowed before <code>character</code> .	For example, <code>"\Bt"</code> matches "t" in "install", but not "t" in "big top".
<code>character1\w</code>	Matches <code>character1character2</code> . <code>character2</code> must be a number, letter, or underline, and <code>\w</code> equals <code>[^A-Za-z0-9_]</code> .	For example, <code>"v\w"</code> matches "vlan", with "v" being <code>character1</code> , and "l" being <code>character2</code> . <code>v\w</code> also matches "service", with "i" being <code>character2</code> .
<code>\W</code>	Equals <code>\b</code> .	For example, <code>"\Wa"</code> matches "a", with "-" being <code>character1</code> , and "a" being <code>character2</code> , but does not match "2a" or "ba".
<code>\</code>	Escape character. If a special character listed in this table follows <code>\</code> , the specific meaning of the character is removed.	For example, <code>"\\"</code> matches a string containing "\", <code>"\^"</code> matches a string containing "^", and <code>"\\b"</code> matches a string containing "\b".

## Example of filtering output information

### 1. Example of using the **begin** keyword

# Display the configuration from the line containing "user-interface" to the last line in the current configuration (the output information depends on the current configuration).

```
<Sysname> display current-configuration | begin user-interface
user-interface aux 0
user-interface vty 0 15
authentication-mode none
```

```

user privilege level 3
#
return

```

## 2. Example of using the **exclude** keyword

# Display the non-direct routes in the routing table (the output depends on the current configuration).

```

<Sysname> display ip routing-table | exclude Direct
Routing Tables: Public

```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
1.1.1.0/24	Static	60	0	192.168.0.0	Vlan1

## 3. Example of using the **include** keyword

# Display the route entries that contain Vlan in the routing table (the output depends on the current configuration).

```

<Sysname> display ip routing-table | include Vlan
Routing Tables: Public

```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
192.168.1.0/24	Direct	0	0	192.168.1.42	Vlan999

# Configuring user privilege and command levels

## Introduction

To avoid unauthorized access, the switch defines user privilege levels and command levels. User privilege levels correspond to command levels. When a user at a specific privilege level logs in, the user can only use commands at that level or lower levels.

All the commands are categorized into four levels: visit, monitor, system, and manage, and are identified from low to high, respectively by 0 through 3. [Table 5](#) describes the command levels.

**Table 5 Default command levels**

Level	Privilege	Description
0	Visit	Involves commands for network diagnosis and accessing an external device. Command configuration at this level cannot survive a device restart. Upon device restart, the commands at this level will be restored to the default settings. Commands at this level include <b>ping</b> , <b>tracert</b> , <b>telnet</b> and <b>ssh2</b> .
1	Monitor	Involves commands for system maintenance and service fault diagnosis. Commands at this level are not allowed to be saved after being configured. After the switch is restarted, the commands at this level will be restored to the default settings. Commands at this level include <b>debugging</b> , <b>terminal</b> , <b>refresh</b> , <b>reset</b> , and <b>send</b> .
2	System	Involves service configuration commands, such as routing configuration commands and commands for configuring services at different network levels. By default, commands at this level include all configuration commands except for those at the manage level.

Level	Privilege	Description
3	Manage	Involves commands that influence the basic operation of the system and commands for configuring system support modules. By default, commands at this level involve the configuration commands of file system, FTP, TFTP, Xmodem download, user management, level setting, and parameter settings within a system (which are not defined by any protocols or RFCs).

## Configuring a user privilege level

A user privilege level can be configured by using AAA authentication parameters or under a user interface.

### Configure user privilege level by using AAA authentication parameters

If the user interface authentication mode is scheme, the user privilege level of users logging into the user interface is specified in AAA authentication configuration.

Follow these steps to configure the user privilege level by using AAA authentication parameters:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enter user interface view	<b>user-interface</b> { <i>first-num1</i> [ <i>last-num1</i> ] }   { <b>aux</b>   <b>vtty</b> } <i>first-num2</i> [ <i>last-num2</i> ] }	—
Specify the scheme authentication mode	<b>authentication-mode scheme</b>	Required By default, the authentication mode for VTY users is <b>password</b> , and no authentication is needed for AUX login users.
Return to system view	<b>quit</b>	—
Configure the authentication mode for SSH users as <b>password</b>	For more information about SSH, see the <i>Security Configuration Guide</i> .	Required if users use SSH to log in, and username and password are needed at authentication
Configure the user privilege level by using AAA authentication parameters	Using local authentication	<ul style="list-style-type: none"> <li>Use the <b>local-user</b> command to create a local user and enter local user view.</li> <li>Use the <b>level</b> keyword in the <b>authorization-attribute</b> command to configure the user privilege level.</li> </ul>
	Using remote authentication (RADIUS, HWTACACS authentications)	Configure the user privilege level on the authentication server  Use either approach <ul style="list-style-type: none"> <li>For local authentication, if you do not configure the user privilege level, the user privilege level is 0.</li> <li>For remote authentication, if you do not configure the user privilege level, the user privilege level depends on the default configuration of the authentication server.</li> </ul>

### Example of configuring a user privilege level by using AAA authentication parameters

# You are required to authenticate the users that Telnet to the switch through VTY 1, verify their username and password, and specify the user privilege level as 3.

```

<Sysname> system-view
[Sysname] user-interface vty 1
[Sysname-ui-vty1] authentication-mode scheme
[Sysname-ui-vty1] quit
[Sysname] local-user test
[Sysname-luser-test] password cipher 12345678
[Sysname-luser-test] service-type telnet

```

When users telnet to the switch through VTY 1, they need to input username **test** and password **12345678**. After passing authentication, the users can only use level 0 commands. If the users want to use commands level 0, 1, 2 and 3 commands, the following configuration is required:

```
[Sysname-luser-test] authorization-attribute level 3
```

## Configure the user privilege level under a user interface

- If the user interface authentication mode is **scheme**, and SSH **publickey** authentication type (only a username is needed for this authentication type) is adopted, the user privilege level of users logging into the user interface is the user interface level.
- If the user interface authentication mode is **none** or **password**, the user privilege level of users logging into the user interface is the user interface level.

Follow these steps to configure the user privilege level under a user interface (SSH **publickey** authentication type):

To do...	Use the command...	Remarks
Configure the authentication type for SSH users as <b>publickey</b>	For more information about SSH, see the <i>Security Configuration Guide</i> .	Required if the SSH login mode is adopted, and only username is needed during authentication. After the configuration, the authentication mode of the corresponding user interface must be set to <b>scheme</b> .
Enter system view	<b>system-view</b>	—
Enter user interface view	<b>user-interface</b> { <i>first-num1</i> [ <i>last-num1</i> ]   <b>vtty</b> <i>first-num2</i> [ <i>last-num2</i> ] }	—
Configure the authentication mode for any user that uses the current user interface to log in to the switch	<b>authentication-mode scheme</b>	Required By default, the authentication mode for VTY users is <b>password</b> , and no authentication is needed for AUX users.
Configure the privilege level for users that log in through the current user interface	<b>user privilege level</b> <i>level</i>	Optional By default, the user privilege level for users logged in through the AUX user interface is 3, and that for users logged in through the VTY interfaces is 0.

Follow these steps to configure the user privilege level under a user interface (**none** or **password** authentication mode):

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enter user interface view	<b>user-interface</b> { <i>first-num 1</i> [ <i>last-num 1</i> ]   { <b>aux</b>   <b>vty</b> } <i>first-num2</i> [ <i>last-num2</i> ] }	—
Configure the authentication mode for any user that uses the current user interface to log in to the switch	<b>authentication-mode</b> { <b>none</b>   <b>password</b> }	Optional By default, the authentication mode for VTY user interfaces is <b>password</b> , and no authentication is needed for AUX login users.
Configure the privilege level of users logged in through the current user interface	<b>user privilege level</b> <i>level</i>	Optional By default, the user privilege level for users logged in through the AUX user interface is 3, and that for users logged in through the VTY interfaces is 0.

### Example of configuring a user privilege level under a user interface

# Authenticate users logged in to the switch through Telnet, verify their password, and specify their user privilege level as 2.

```
<Sysname> system-view
[Sysname] user-interface vty 0 15
[Sysname-ui-vty0-15] authentication-mode password
[Sysname-ui-vty0-15] set authentication password cipher 123
[Sysname-ui-vty0-15] user privilege level 2
```

By default, Telnet users can use level 0 commands after passing authentication. After the configuration above is completed, when users log in to the switch through Telnet, they need to input password **123**, and then they can use level 0, 1, and 2 commands.

#### NOTE:

- For more information about user interfaces, see the chapter “Logging in to the switch configuration.” For more information about the **user-interface**, **authentication-mode**, and **user privilege level** commands, see the chapter “Logging in to the switch commands.”
- For more information about AAA authentication, see the *Security Configuration Guide*. For more information about the **local-user** and **authorization-attribute** commands, see the *Security Command Reference*.
- For more information about SSH, see the *Security Configuration Guide*.

## Switching user privilege level

### Introduction

Users can switch to a different user privilege level temporarily without logging out and terminating the current connection. After the privilege level switch, users can continue to configure the switch without the need to logging back in, but the commands that they can execute have changed. For example, if the current user privilege level is 3, the user can configure system parameters. After switching to user privilege level 0, the user can only execute simple commands, like **ping** and **tracert**, and only a few

**display** commands. The switching operation is effective for the current login. After the user logs back in, the user privilege restores to the original level.

- To avoid problems, HP recommends that administrators log in to the switch by using a lower privilege level and view switch operating parameters. To maintain the switch, administrators can temporarily switch to a higher level.
- If the administrators need to leave or need to ask someone else to temporarily manage the switch, they can switch to a lower privilege level to restrict the operation by others.

### Setting the authentication mode for user privilege level switch

- A user can switch to a privilege level equal to or lower than the current one unconditionally and is not required to input a password (if any).
- For security, a user is required to input the password (if any) to switch to a higher privilege level. The authentication falls into one of the following four categories:

Authentication mode	Meaning	Description
<b>local</b>	Local password authentication	The switch authenticates a user by using the privilege level switch password input by the user. When this mode is applied, you need to set the password for privilege level switch with the <b>super password</b> command.
<b>scheme</b>	Remote AAA authentication through HWTACACS or RADIUS	The switch sends the username and password for privilege level switch to the HWTACACS or RADIUS server for remote authentication. When this mode is applied, you need to perform the following configurations: <ul style="list-style-type: none"> <li>• Configure HWTACACS or RADIUS scheme and reference the created scheme in the ISP domain. For more information, see the <i>Security Configuration Guide</i>.</li> <li>• Create the corresponding user and configure password on the HWTACACS or RADIUS server.</li> </ul>
<b>local scheme</b>	Performs the local password authentication first and then the remote AAA authentication	The switch authenticates a user by using the local password first. If no local password is set, the privilege level is switched directly for the users logged in from the AUX port, and remote AAA authentication is performed on the users logged in from VTY user interfaces.
<b>scheme local</b>	Performs remote AAA authentication first and then the local password authentication	AAA authentication is performed first, and if the remote HWTACACS or RADIUS server does not respond or AAA configuration on the switch is invalid, the local password authentication is performed.

Follow these steps to set the authentication mode for user privilege level switch:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Set the authentication mode for user privilege level switch	<b>super authentication-mode { local   scheme } *</b>	Optional <b>local</b> by default.



To do...	Use the command...	Remarks
Configure the password for user privilege level switch	<b>super password</b> [ <b>level</b> <i>user-level</i> ] { <b>simple</b>   <b>cipher</b> } <i>password</i>	Required if the authentication mode is set to <b>local</b> . By default, no privilege level switch password is configured.

**△ CAUTION:**

- If no user privilege level is specified when you configure the password for switching the user privilege level with the **super password** command, the user privilege level defaults to 3.
- Specifying the **simple** keyword saves the password in plain text, which is less secure than specifying the **cipher** keyword, which saves the password in cipher text.
- If the user logs in from the AUX user interface (the console port), the user can switch the privilege level to a higher level even if the authentication mode is **local** and no password for user privilege level switch is configured.

### Switching the user privilege level

Follow the step to switch the user privilege level:

To do...	Use the command...	Remarks
Switch the user privilege level	<b>super</b> [ <i>level</i> ]	Required When logging in to the switch, a user has a user privilege level, which depends on user interface or authentication user level. Available in user view.

When you switch the user privilege level, the information you need to provide varies with combinations of the user interface authentication mode and the super authentication mode.

**Table 6 Information input for user privilege level switch**

User interface authentication mode	User privilege level switch authentication mode	Information input for the first authentication mode	Information input after the authentication mode changes
none/password	<b>local</b>	Local user privilege level switch password (configured on the switch)	—
	<b>local scheme</b>	Local user privilege level switch password	Username and password for privilege level switch (configured on the AAA server)
	<b>scheme</b>	Username and password for privilege level switch	—
	<b>scheme local</b>	Username and password for privilege level switch	Local user privilege level switch password

User interface authentication mode	User privilege level switch authentication mode	Information input for the first authentication mode	Information input after the authentication mode changes
<b>scheme</b>	<b>local</b>	Local user privilege level switch password	—
	<b>local scheme</b>	Local user privilege level switch password	Password for privilege level switch (configured on the AAA server). The system uses the username used for logging in as the privilege level switch username.
	<b>scheme</b>	Password for privilege level switch (configured on the AAA server). The system uses the username used for logging in as the privilege level switch username.	—
	<b>scheme local</b>	Password for privilege level switch (configured on the AAA server). The system uses the username used for logging in as the privilege level switch username.	Local user privilege level switch password

**△ CAUTION:**

- When the authentication mode is set to **local**, configure the local password before switching to a higher user privilege level.
- When the authentication mode is set to **scheme**, configure AAA related parameters before switching to a higher user privilege level.
- The privilege level switch fails after three consecutive unsuccessful password attempts.
- For more information about user interface authentication, see the chapter “Logging in to the switch configuration.”

## Modifying the level of a command

All the commands in a view default to different levels. The administrator can change the default level of a command to a different level as needed.

Follow these steps to modify the command level:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Configure the command level in a specified view	<b>command-privilege level level/ view view command</b>	Required See <a href="#">Table 5</a> for the default settings.

---

 **CAUTION:**

HP recommends that you use the default command level or modify the command level under the guidance of professional staff. An improper change of the command level may bring inconvenience to your maintenance and operation, or even potential security problems.

---

## Saving the current configuration

On the device, you can input the **save** command in any view to save all of the submitted and executed commands into the configuration file. Commands saved in the configuration file can survive a reboot. The **save** command does not take effect on one-time commands, such as **display** commands, which display specified information, and the **reset** commands, which clear specified information. One-time commands that are executed are never saved.

## Displaying and maintaining CLI

To do...	Use the command...	Remarks
Display defined command aliases and the corresponding commands	<b>display command-alias</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display the clipboard information	<b>display clipboard</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view

# Login methods

## Login methods

You can log in to the switch by using the following methods.

**Table 7 Login methods**

Login method	Default state
CLI login	Logging in through the console port By default, you can log in to a device through the console port, the authentication mode is None (no username or password required), and the user privilege level is 3.
	Logging in through By default, you cannot log in to a device through Telnet. To do so, log in to the device through the console port, and complete the following configuration: <ul style="list-style-type: none"><li>• Enable the Telnet function.</li><li>• Configure the IP address of the VLAN interface, and make sure that your device and the Telnet client can reach each other (by default, the device does not have an IP address.).</li><li>• Configure the authentication mode of VTY login users (password by default).</li><li>• Configure the user privilege level of VTY login users (0 by default).</li></ul>
	Logging in through SSH By default, you cannot log in to a device through SSH. To do so, log in to the device through the console port, and complete the following configuration: <ul style="list-style-type: none"><li>• Enable the SSH function and configure SSH attributes.</li><li>• Configure the IP address of the VLAN interface, and make sure that your device and the SSH client can reach each other (by default, your device does not have an IP address.).</li><li>• Configure the authentication mode of VTY login users as <b>scheme</b> (password by default).</li><li>• Configure the user privilege level of VTY login users (0 by default).</li></ul>
Web login	Logging in through modems By default, you can log in to a device through modems. The default user privilege level of modem login users is 3.
	By default, you cannot log in to a device through web. To do so, log in to the device through the console port, and complete the following configuration: <ul style="list-style-type: none"><li>• Configure the IP address of the VLAN interface (by default, your device does not have an IP address.).</li><li>• Configure a username and password for web login (not configured by default).</li><li>• Configure the user privilege level for web login (not configured by default).</li><li>• Configure the Telnet service type for web login (not configured by default).</li></ul>

Login method	Default state
NMS login	<p>By default, you cannot log in to a device through a network management system (NMS). To do so, log in to the device through the console port, and complete the following configuration:</p> <ul style="list-style-type: none"> <li>• Configure the IP address of the VLAN interface, and make sure the device and the NMS can reach each other (by default, your device does not have an IP address.).</li> <li>• Configure SNMP basic parameters.</li> </ul>

## User interface overview

User interface, also called “*line*”, allows you to manage and monitor sessions between the terminal and device when you log in to the device through the console port directly, or through Telnet or SSH.

One user interface corresponds to one user interface view where you can configure a set of parameters, such as whether to authenticate users at login, whether to redirect the requests to another device, and the user privilege level after login. When the user logs in through a user interface, the parameters set for the user interface apply.

The system supports the following CLI configuration methods:

- Local configuration via the console port
- Local/Remote configuration through Telnet or SSH

The methods correspond to the following user interfaces.

- AUX user interface: Used to manage and monitor user that log in via the Console port. The type of the Console port is EIA/TIA-232 DCE.
- VTY (virtual type terminal) user interface: Used to manage and monitor users that log in via VTY. A VTY port used for Telnet or SSH access.

## Users and user interfaces

Only one user can use a user interface at a time. The configuration made in a user interface view applies to any login user. For example, if user A uses the console port to log in, the configuration in the AUX user interface view applies to user A; if user A logs in through VTY 1, the configuration in VTY 1 user interface view applies to user A.

A device can be equipped with one AUX user interface and 16 VTY user interfaces. These user interfaces are not associated with specific users. When a user initiates a connection request, the system automatically assigns the idle user interface with the smallest number to the user based on the login method. During the login, the configuration in the user interface view takes effect. The user interface varies depending on the login method and the login time.

## Numbering user interfaces

User interfaces can be numbered by using absolute numbering or relative numbering.

### Absolute numbering

Absolute numbering identifies a user interface or a group of different types of user interfaces. The specified user interfaces are numbered from number 0 with a step of 1 and in the sequence of AUX, and

VTY user interfaces. You can use the **display user-interface** command without any parameters to view supported user interfaces and their absolute numbers.

### Relative numbering

Relative numbering allows you to specify a user interface or a group of user interfaces of a specific type. The number format is “user interface type + number”. The following rules of relative numbering apply:

- AUX user interfaces are numbered from 0 in the ascending order, with a step of 1.
- VTY user interfaces are numbered from 0 in the ascending order, with a step of 1.

---

# CLI login

## Overview

The CLI enables you to interact with a device by typing text commands. At the CLI, you can instruct your device to perform a given task by typing a text command and then pressing **Enter** to submit it to your device. Compared with a GUI, where you can use a mouse to perform configuration, the CLI allows you to input more information in one command line.

You can log in to the device at the CLI through the console port, Telnet, SSH, or modem.

- By default, you can log in to a device through the console port without any authentication, which introduces security problems.
- By default, you cannot log in to a device through Telnet, SSH, so you cannot remotely manage and maintain the device.

Therefore, you need to perform configurations to increase device security and manageability.

## Logging in through the console port

### Introduction

Logging in through the console port is the most common login method, and is also the first step to configure other login methods.

After logging in to the device through the console port, you can configure other login methods. By default, you can log in to a device only through its console port.

This section includes:

- [Configuration requirements](#)
- [Login procedure](#)
- [Console login authentication modes](#)
- [Configuring none authentication for console login](#)
- [Configuring password authentication for console login](#)
- [Configuring scheme authentication for console login](#)
- [Configuring common settings for console login \(optional\)](#)

### Configuration requirements

The following table shows the configuration requirements for console port login.

<b>Object</b>	<b>Requirements</b>
Device	No configuration requirement
Terminal	Run the hyper terminal program.
	Configure the hyper terminal attributes.

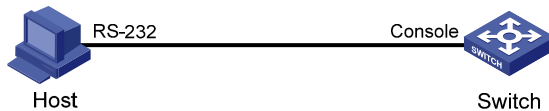
The port properties of the hyper terminal must be the same as the default settings of the console port shown in the following table.

Setting	Default
Bits per second	9,600 bps
Flow control	None
Parity	None
Stop bits	1
Data bits	8

## Login procedure

- Step1** Use the console cable shipped with the device to connect the PC and the device. Plug the DB-9 connector of the console cable into the serial port of the PC, and plug the RJ-45 connector into the console port of your device.

**Figure 4** Connect the device and PC through a console cable



### **WARNING!**

Identify interfaces to avoid connection errors.

### **NOTE:**

The serial port of a PC does not support hot-swap, so do not plug or unplug the console cable into or from the PC when your device is powered on. To connect the PC to the device, first plug the DB-9 connector of the console cable into the PC, and then plug the RJ-45 connector of the console cable into your device. To disconnect the PC from the device, first unplug the RJ-45 connector and then the DB-9 connector.

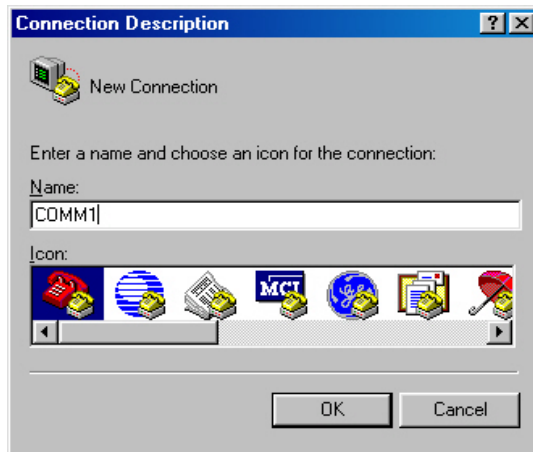
- Step2** Launch a terminal emulation program (such as HyperTerminal in Windows XP/Windows 2000). The following takes Windows XP's HyperTerminal as an example. Select a serial port to be connected to the device, and set terminal parameters as follows: set **Bits per second** to **9600**, **Data bits** to **8**, **Parity** to **None**, **Stop bits** to **1**, and **Flow control** to **None**, as shown in [Figure 5](#) through [Figure 7](#).

### **NOTE:**

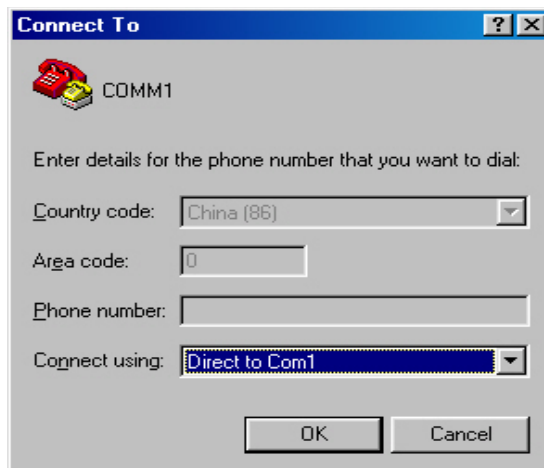
On Windows 2003 Server operating system, you need to add the HyperTerminal program first, and then log in to and manage the device as described in this document. On Windows 2008 Server, Windows 7, Windows Vista, or some other operating system, you need to obtain a third party terminal control program first, and follow the user guide or online help of that program to log in to the device.



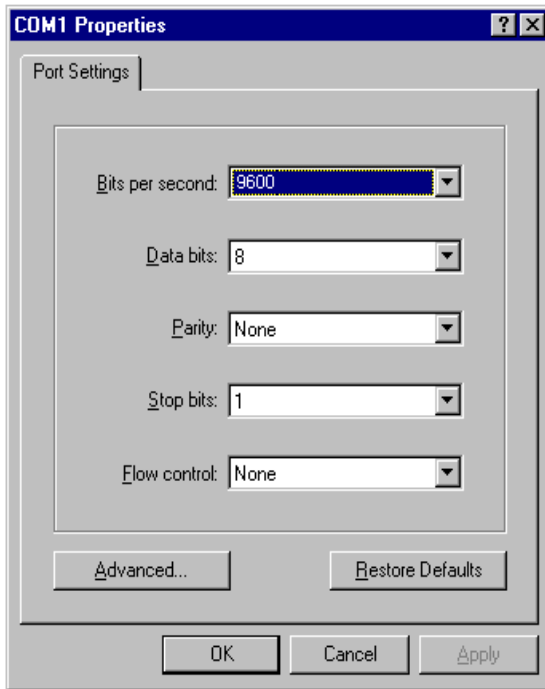
**Figure 5 Connection description**



**Figure 6 Specify the serial port used to establish the connection**

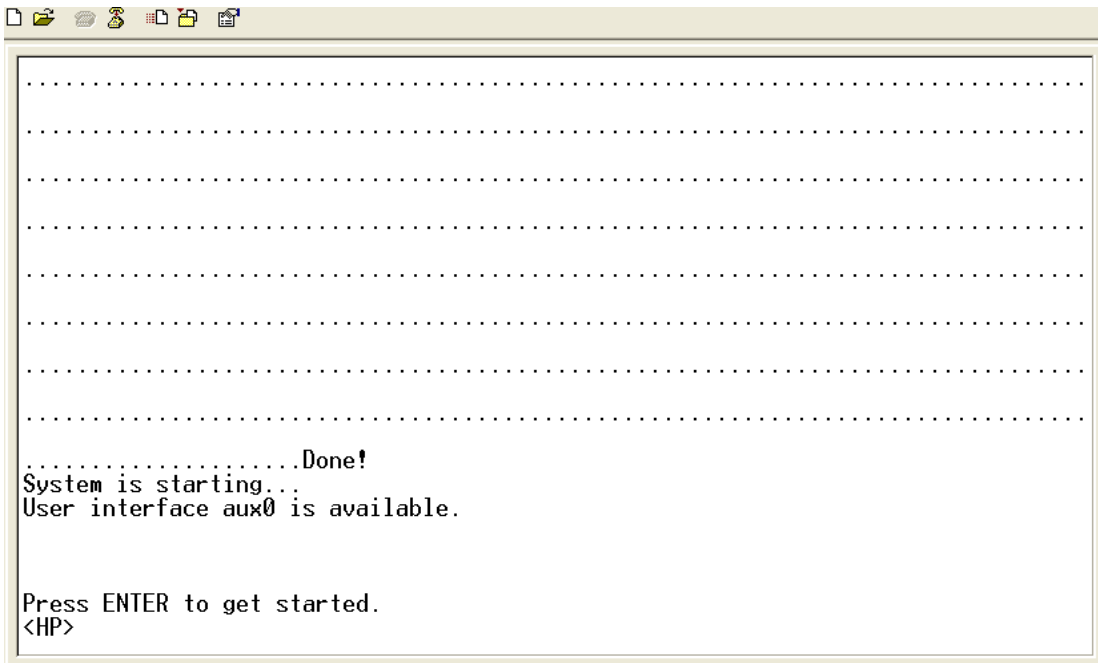


**Figure 7 Set the properties of the serial port**



**Step3** Turn on the device. You are prompted to press **Enter** if the device successfully completes the power-on self test (POST). A prompt such as <HP> appears after you press **Enter**, as shown in [Figure 8](#).

**Figure 8 Configuration page**



**Step4** Execute commands to configure the device or check the running status of the device. To get help, type ?.

## Console login authentication modes

The following authentication modes are available for console port login: **none**, **password**, and **scheme**.

- **none**—Requires no username and password at the next login through the console port. This mode is insecure.
- **password**—Requires password authentication at the next login through the console port. Keep your password.
- **scheme**—Requires username and password authentication at the next login through the console port. Authentication falls into local authentication and remote authentication. To use local authentication, configure a local user and related parameters. To use remote authentication, configure the username and password on the remote authentication server. For more information about authentication modes and parameters, see the *Security Configuration Guide*.

The following table lists console port login configurations for different authentication modes:

Authentication mode	Configuration	Remarks	
None	Configure not to authenticate users	For more information, see <a href="#">“Configuring none authentication for console login.”</a>	
Password	Configure to authenticate users by using the local password	For more information, see <a href="#">“Configuring password authentication for console login.”</a>	
	Set the local password		
Scheme	Configure the authentication scheme		
	Select an authentication scheme	Remote AAA authentication	Configure a RADIUS/HWTACACS scheme
			Configure the AAA scheme used by the domain
		Local authentication	Configure the authentication username and password
		Configure the AAA scheme used by the domain as local	

**NOTE:**

A newly configured authentication mode does not take effect unless you exit and enter the CLI again.

## Configuring none authentication for console login

### Configuration prerequisites

You have logged in to the device.

By default, you can log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see [“Configuration requirements.”](#)

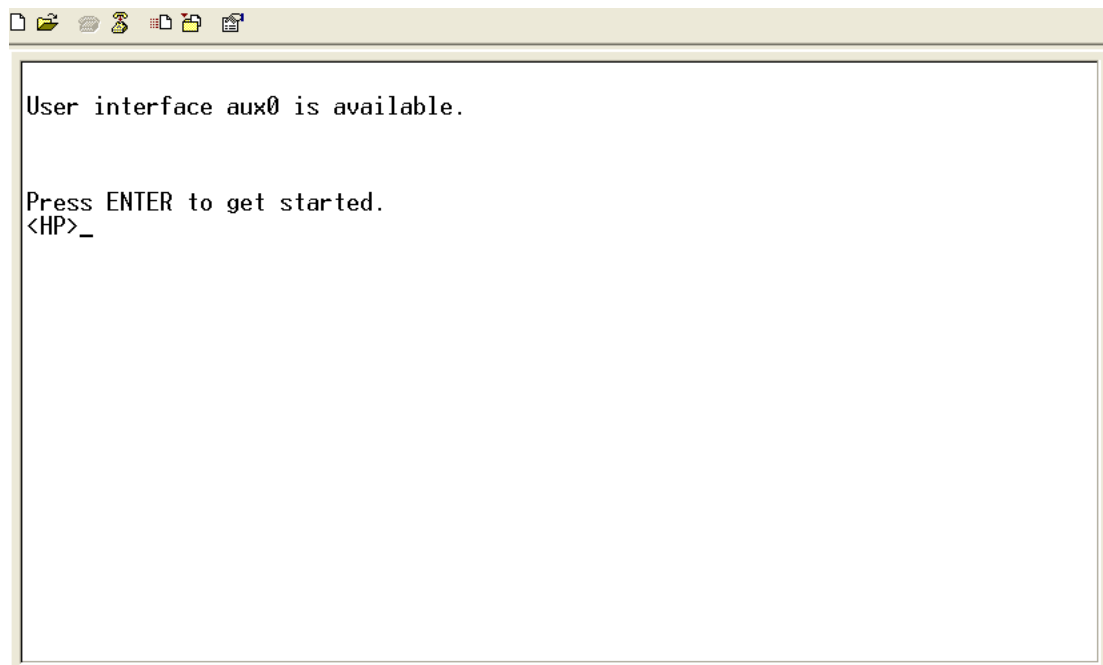
## Configuration procedure

Follow these steps to configure none authentication for console login:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enter AUX user interface view	<b>user-interface aux</b> <i>first-number</i> [ <i>last-number</i> ]	—
Specify the none authentication mode	<b>authentication-mode none</b>	Required By default, you can log in to the device through the console port without authentication, and have user privilege level 3 after login.
Configure common settings for AUX user interface view	—	Optional See <a href="#">“Configuring common settings for console login (optional).”</a>

After the configuration, the next time you log in to the device through the console port, you are prompted to press **Enter**. A prompt such as <HP> appears after you press **Enter**, as shown in [Figure 9](#).

**Figure 9 Configuration page**



## Configuring password authentication for console login

### Configuration prerequisites

You have logged in to the device.

By default, you can log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see [“Configuration requirements.”](#)

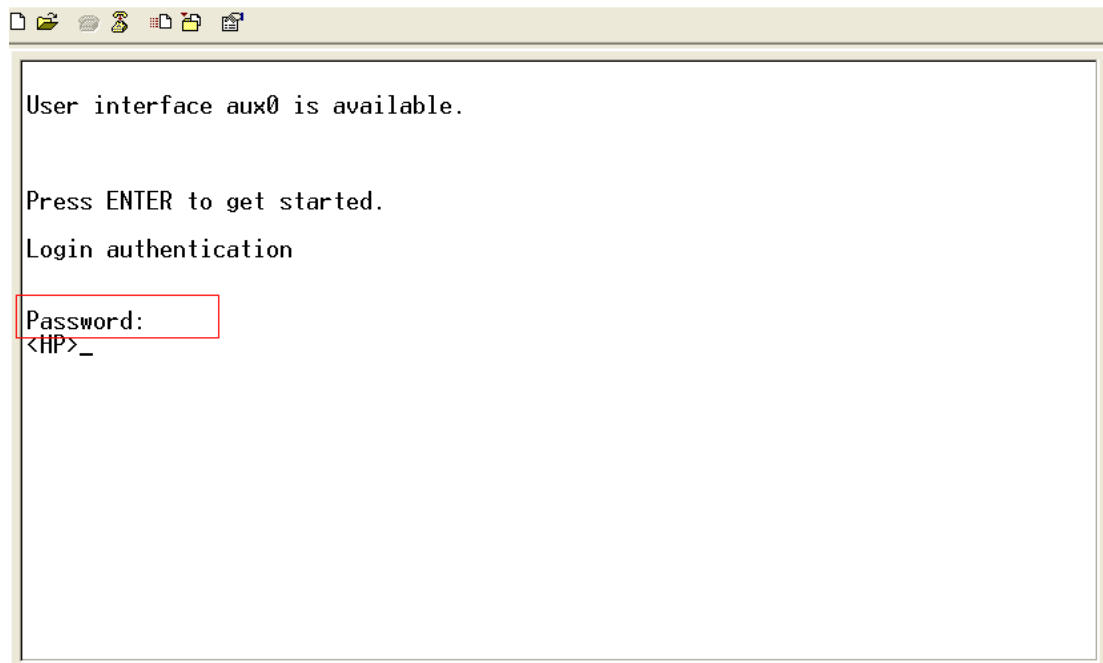
## Configuration procedure

Follow these steps to configure password authentication for console login:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enter AUX user interface view	<b>user-interface aux</b> <i>first-number</i> [ <i>last-number</i> ]	—
Configure the authentication mode as local password authentication	<b>authentication-mode password</b>	Required By default, you can log in to the device through the console port without authentication and have user privilege level 3 after login.
Set the local password	<b>set authentication password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	Required By default, no local password is set.
Configure common settings for AUX user interface view	—	Optional See <a href="#">“Configuring common settings for console login (optional).”</a>

When you log in to the device through the console port after configuration, you are prompted to enter a login password. A prompt such as <HP> appears after you input the password and press **Enter**, as shown in [Figure 10](#).

**Figure 10 Configuration page**



# Configuring scheme authentication for console login

## Configuration prerequisites

You have logged in to the device.

By default, you can log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “[Configuration requirements](#).”

## Configuration procedure

Follow these steps to configure scheme authentication for console login:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enter AUX user interface view	<b>user-interface aux</b> <i>first-number</i> [ <i>last-number</i> ]	—
Specify the scheme authentication mode	<b>authentication-mode scheme</b>	Required Whether local, RADIUS, or HWTACACS authentication is adopted depends on the configured AAA scheme. By default, users that log in through the console port are not authenticated.
Enable command authorization	<b>command authorization</b>	Optional <ul style="list-style-type: none"><li>By default, command authorization is not enabled.</li><li>By default, the command level depends on the user privilege level. A user is authorized a command level not higher than the user privilege level. With command authorization enabled, the command level for a login user is determined by both the user privilege level and AAA authorization. If a user executes a command of the corresponding command level, the authorization server checks whether the command is authorized. If yes, the command can be executed.</li><li>Before enabling command authorization, configure the AAA authorization server. After you enable command authorization, only commands authorized by the AAA authorization server can be executed.</li></ul>

To do...	Use the command...	Remarks
Enable command accounting	<b>command accounting</b>	<p>Optional</p> <ul style="list-style-type: none"> <li>By default, command accounting is disabled. The accounting server does not record the commands executed by users.</li> <li>Command accounting allows the HWTACACS server to record all the commands executed by users, regardless of command execution results. This helps control and monitor user operations on the device. If command accounting is enabled and command authorization is not enabled, every executed command is recorded on the HWTACACS server. If both command accounting and command authorization are enabled, only the authorized and executed commands are recorded on the HWTACACS server.</li> <li>Configure the AAA accounting server before enabling command accounting.</li> </ul>
Return to system view	<b>quit</b>	—
Enter the ISP domain view	<b>domain</b> <i>domain-name</i>	Optional
Apply the specified AAA scheme to the domain	<b>authentication default</b> { <b>hwtacacs-scheme</b> <i>hwtacacs-scheme-name</i> [ <b>local</b> ]   <b>local</b>   <b>none</b>   <b>radius-scheme</b> <i>radius-scheme-name</i> [ <b>local</b> ] }	<p>By default, the AAA scheme is <b>local</b>.</p> <p>If you specify the local AAA scheme, you need to perform local user configuration. If you specify an existing scheme by providing the <i>radius-scheme-name</i> argument, perform the following configuration as well:</p> <ul style="list-style-type: none"> <li>For RADIUS and HWTACACS configuration, see the <i>Security Configuration Guide</i>.</li> <li>Configure the username and password on the AAA server. (For more information about AAA, see the <i>Security Configuration Guide</i>.)</li> </ul>
Configure the authentication mode		
Exit to system view	<b>quit</b>	
Create a local user and enter local user view	<b>local-user</b> <i>user-name</i>	<p>Required</p> <p>By default, no local user exists.</p>
Set the authentication password for the local user	<b>password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	Required
Specify the command level of the local user	<b>authorization-attribute level</b> <i>level</i>	<p>Optional</p> <p>By default, the command level is 0.</p>

To do...	Use the command...	Remarks
Specify the service type for the local user	<b>service-type terminal</b>	Required By default, no service type is specified.
Configure common settings for AUX user interface view	—	Optional See <a href="#">“Configuring common settings for console login (optional).”</a>

After you enable command authorization, you need to perform the following configuration to make the function take effect:

- Create a HWTACACS scheme, and specify the IP address of the authorization server and other authorization parameters. For more information about AAA, see the *Security Configuration Guide*.
- Reference the created HWTACACS scheme in the ISP domain. For more information about AAA, see the *Security Configuration Guide*.

After you enable command accounting, you need to perform the following configuration to make the function take effect:

- Create a HWTACACS scheme, and specify the IP address of the accounting server and other accounting parameters. For more information about AAA, see the *Security Configuration Guide*.
- Reference the created HWTACACS scheme in the ISP domain. For more information about AAA, see the *Security Configuration Guide*.

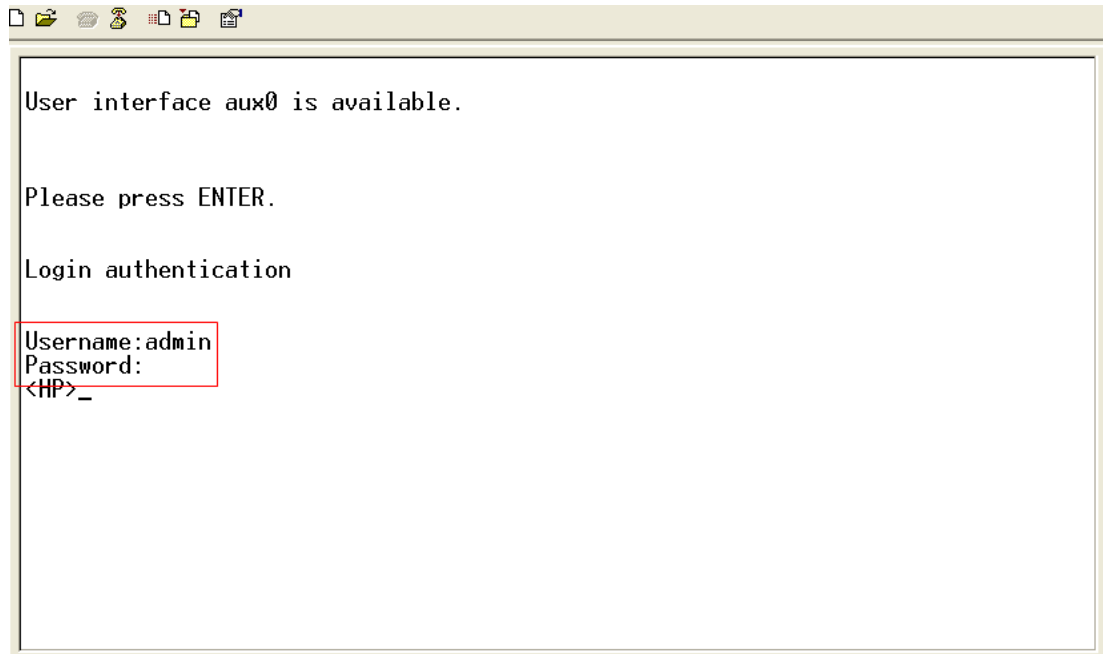
When users adopt the scheme mode to log in to the device, the level of the commands that the users can access depends on the user privilege level defined in the AAA scheme.

- When the AAA scheme is local, the user privilege level is defined by the **authorization-attribute level level** command.
- When the AAA scheme is RADIUS or HWTACACS, the user privilege level is configured on the RADIUS or HWTACACS server.
- For more information about AAA, RADIUS, and HWTACACS, see the *Security Configuration Guide*.

When you log in to the device through the console port after the configuration, you are prompted to enter a login username and password. A prompt such as <HP> appears after you input the password and username and press **Enter**, as shown in [Figure 11](#).



Figure 11 Configuration page



## Configuring common settings for console login (optional)

Follow these steps to configure common settings for console port login

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enable display of copyright information	<b>copyright-info enable</b>	Optional Enabled by default.
Enter AUX user interface view	<b>user-interface aux</b> <i>first-number</i> [ <i>last-number</i> ]	—
Configure AUX user interface view properties	Configure the baud rate	Optional By default, the transmission rate is 9600 bps. Transmission rate is the number of bits that the device transmits to the terminal per second.
	Configure the parity check mode	Optional <b>parity</b> { <b>even</b>   <b>none</b>   <b>odd</b> } <b>none</b> by default.
	Configure the stop bits	Optional By default, the stop bits of the console port is 1. Stop bits are the last bits transmitted in data transmission to unequivocally indicate the end of a character. The more the bits are, the slower the transmission is.

To do...	Use the command...	Remarks
Configure the data bits	<b> databits { 5   6   7   8 }</b>	Optional By default, the data bits of the console port is 8. Data bits is the number of bits representing one character. The setting depends on the contexts to be transmitted. For example, you can set it to 7 if standard ASCII characters are to be sent, and set it to 8 if extended ASCII characters are to be sent.
Define a shortcut key for enabling a terminal session	<b> activation-key </b> <i>character</i>	Optional By default, you can press <b>Enter</b> to enable a terminal session.
Define a shortcut key for terminating tasks	<b> escape-key { default   character }</b>	Optional By default, you can press <b>Ctrl+C</b> to terminate a task.
Configure the flow control mode	<b> flow-control { hardware   none   software }</b>	Optional By default, the value is <b>none</b>
Configure the type of terminal display	<b> terminal type { ansi   vt100 }</b>	Optional By default, the terminal display type is ANSI. The device supports two types of terminal display: ANSI and VT100. HP recommends that you set the display type of both the device and the client to VT100. If the device and the client use different display types (for example, hyper terminal or Telnet terminal) or both are set to ANSI, when the total number of characters of the edited command line exceeds 80, an anomaly such as cursor corruption or abnormal display of the terminal display may occur on the client.
Configure the user privilege level for login users	<b> user privilege level </b> <i>level</i>	Optional By default, the default command level is 3 for the AUX user interface.
Set the maximum number of lines on the next screen.	<b> screen-length </b> <i>screen-length</i>	Optional By default, the next screen displays 24 lines. A value of 0 disables the function.
Set the size of history command buffer	<b> history-command max-size </b> <i>value</i>	Optional By default, the buffer saves 10 history commands at most.

To do...	Use the command...	Remarks
Set the idle-timeout timer	<b>idle-timeout</b> <i>minutes</i> [ <i>seconds</i> ]	Optional The default idle-timeout is 10 minutes. The system automatically terminates the user's connection if no information interaction occurs between the device and the user within the idle-timeout time. Setting idle-timeout to 0 disables the timer.

**CAUTION:**

The common settings configured for console login take effect immediately. If you configure the common settings after you log in through the console port, the current connection may be interrupted, so you must use another login method. After you configure common settings for console login, you need to modify the settings on the terminal to make them consistent with those on the device.

# Logging in through Telnet

## Introduction

The device supports Telnet. You can Telnet to the device to remotely manage and maintain it, as shown in Figure 12.

**Figure 12 Telnet login**



The following table shows the configuration requirements of Telnet login.

Object	Requirements
Telnet server	Configure the IP address of the VLAN interface, and make sure the Telnet server and client can reach each other.
	Configure the authentication mode and other settings
Telnet client	Run the Telnet client program.
	Obtain the IP address of the VLAN interface on the server

By default, the device is enabled with the Telnet server and client functions.

- On a device that serves as the Telnet client, you can log in to a Telnet server to perform operations on the server.
- On a device that serves as the Telnet server, you can configure the authentication mode and user privilege level for Telnet users. By default, you cannot log in to the device through Telnet. Before you can Telnet to the device, you need to log in to the device through the console port, enable Telnet server, and configure the authentication mode, user privilege level, and common settings.

This section includes these topics:

- [Telnet login authentication modes](#)
- [Configuring none authentication for Telnet login](#)
- [Configuring password authentication for Telnet login](#)
- [Configuring scheme authentication for Telnet login](#)
- [Configuring common settings for VTY user interfaces \(optional\)](#)
- [Configuring the device to log in to a Telnet server as a Telnet client](#)

## Telnet login authentication modes

Three authentication modes are available for Telnet login: **none**, **password**, and **scheme**.

- **none**—Requires no username and password at the next login through Telnet. This mode is insecure.
- **password**—Requires password authentication at the next login through Telnet. Keep your password. If you lose your password, log in to the device through the console port to view or modify the password.
- **scheme**—Requires username and password authentication at the next login through Telnet. Authentication falls into local authentication and remote authentication. To use local authentication, configure a local user and related parameters. To use remote authentication, configure the username and password on the remote authentication server. For more information about authentication modes and parameters, see the *Security Configuration Guide*. Keep your username and password. If you lose your local authentication password, log in to the device through the console port to view or modify the password. If you lose your remote authentication password, contact the administrator.

The following table lists Telnet login configurations for different authentication modes.

Authentication mode	Configuration	Remarks
None	Configure not to authenticate users	For more information, see <a href="#">“Configuring none authentication for Telnet login.”</a>
Password	Configure to authenticate users by using the local password	For more information, see <a href="#">“Configuring password authentication for Telnet login.”</a>
	Set the local password	

Authentication mode	Configuration	Remarks	
	Configure the authentication scheme		
Scheme	Select an authentication scheme	Configure a RADIUS/HWTACACS scheme	For more information, see <a href="#">“Configuring scheme authentication for Telnet login.”</a>
		Remote AAA authentication	
	Local authentication	Configure the authentication username and password	
		Configure the AAA scheme used by the domain as local	

## Configuring none authentication for Telnet login

### Configuration prerequisites

You have logged in to the device.

By default, you can log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see [“Configuration requirements.”](#)

### Configuration procedure

Follow these steps to configure none authentication for Telnet login:

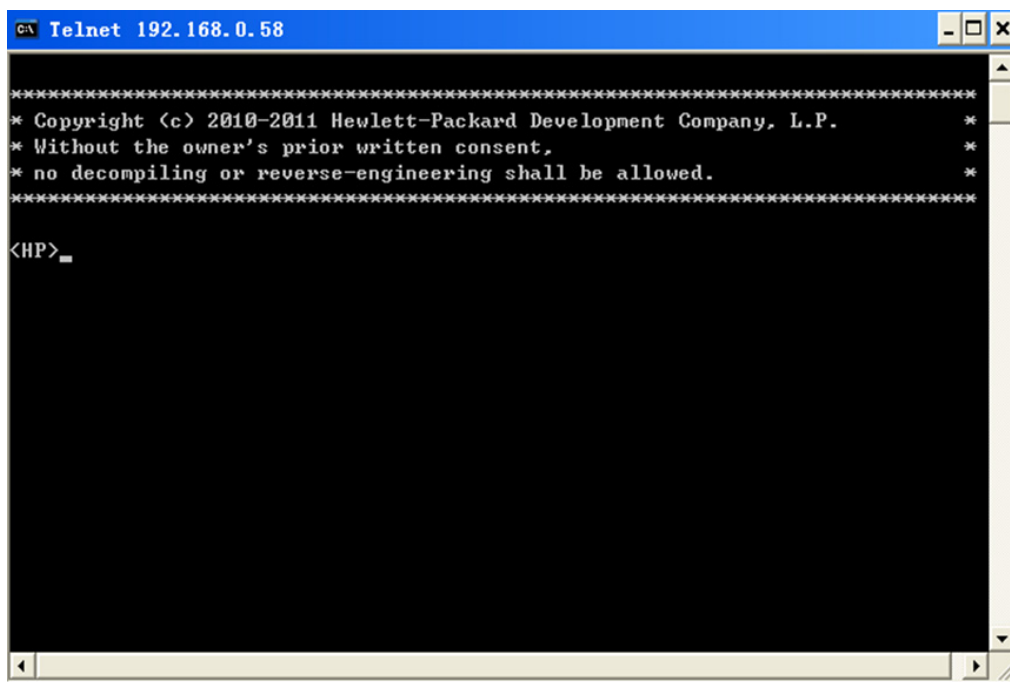
To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enable Telnet	<b>telnet server enable</b>	Required By default, the Telnet service is disabled.
Enter one or multiple VTY user interface views	<b>user-interface vty</b> <i>first-number</i> [ <i>last-number</i> ]	—
Specify the none authentication mode	<b>authentication-mode none</b>	Required By default, authentication mode for VTY user interfaces is <b>password</b> .
Configure the command level for login users on the current user interfaces	<b>user privilege level</b> <i>level</i>	Required By default, the default command level is 0 for VTY user interfaces.

To do...	Use the command...	Remarks
Configure common settings for VTY user interfaces	—	Optional See “ <a href="#">Configuring common settings for VTY user interfaces (optional)</a> .”

When you log in to the device through Telnet again:

- You enter the VTY user interface, as shown in [Figure 13](#).
- If “All user interfaces are used, please try later!” is displayed, it means the current login users exceed the maximum number. Please try later.

**Figure 13 Configuration page**



## Configuring password authentication for Telnet login

### Configuration prerequisites

You have logged in to the device.

By default, you can log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “[Configuration requirements](#).”

### Configuration procedure

Follow these steps to configure password authentication for Telnet login:

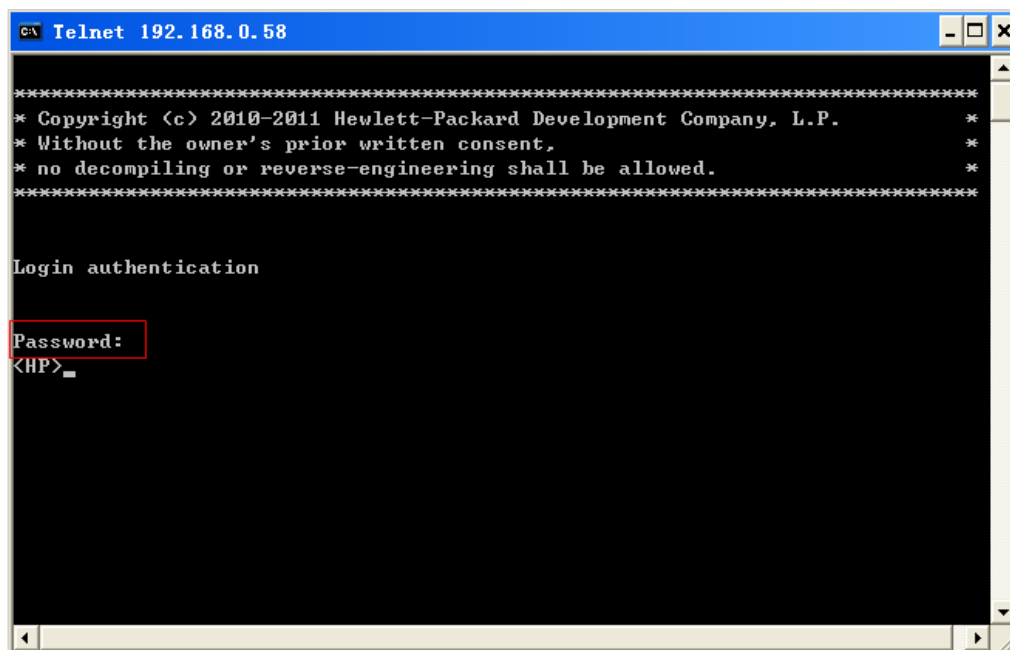
To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enable Telnet	<b>telnet server enable</b>	Required By default, the Telnet service is disabled.

To do...	Use the command...	Remarks
Enter one or multiple VTY user interface views	<b>user-interface vty</b> <i>first-number</i> [ <i>last-number</i> ]	—
Specify the password authentication mode	<b>authentication-mode password</b>	Required By default, authentication mode for VTY user interfaces is <b>password</b> .
Set the local password	<b>set authentication password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	Required By default, no local password is set.
Configure the user privilege level for login users	<b>user privilege level</b> <i>level</i>	Required 0 by default.
Configure common settings for VTY user interfaces	—	Optional See <a href="#">“Configuring common settings for VTY user interfaces (optional).”</a>

When you log in to the device through Telnet again:

- You are required to enter the login password. A prompt such as <HP> appears after you enter the correct password and press **Enter**, as shown in [Figure 14](#).
- If “All user interfaces are used, please try later!” is displayed, it means the number of current concurrent login users exceed the maximum. Please try later.

**Figure 14 Configuration page**



# Configuring scheme authentication for Telnet login

## Configuration prerequisites

You have logged in to the device.

By default, you can log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “[Configuration requirements.](#)”

## Configuration procedure

Follow these steps to configure scheme authentication for Telnet login

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enable Telnet	<b>telnet server enable</b>	Required By default, the Telnet service is disabled.
Enter one or multiple VTY user interface views	<b>user-interface vty</b> <i>first-number</i> [ <i>last-number</i> ]	—
Specify the scheme authentication mode	<b>authentication-mode scheme</b>	Required Whether local, RADIUS, or HWTACACS authentication is adopted depends on the configured AAA scheme. By default, local authentication is adopted.



To do...	Use the command...	Remarks
Enable command authorization	<b>command authorization</b>	<p>Optional</p> <ul style="list-style-type: none"> <li>• By default, command authorization is not enabled.</li> <li>• By default, the command level depends on the user privilege level. A user is authorized a command level not higher than the user privilege level. With command authorization enabled, the command level for a login user is determined by both the user privilege level and AAA authorization. If a user executes a command of the corresponding command level, the authorization server checks whether the command is authorized. If yes, the command can be executed.</li> <li>• Before enabling command authorization, configure the AAA authorization server. After you enable command authorization, only commands authorized by the AAA authorization server can be executed.</li> </ul>

To do...	Use the command...	Remarks
Enable command accounting	<b>command accounting</b>	<p>Optional</p> <ul style="list-style-type: none"> <li>By default, command accounting is disabled. The accounting server does not record the commands executed by users.</li> <li>Command accounting allows the HWTACACS server to record all executed commands that are supported by the device, regardless of the command execution result. This helps control and monitor user operations on the device. If command accounting is enabled and command authorization is not enabled, every executed command is recorded on the HWTACACS server. If both command accounting and command authorization are enabled, only the authorized and executed commands are recorded on the HWTACACS server.</li> <li>Configure the AAA accounting server before enabling command accounting.</li> </ul>
Exit to system view	<b>quit</b>	—
Configure the authentication mode	Enter the default ISP domain view <b>domain</b> <i>domain-name</i>	Optional By default, the AAA scheme is <b>local</b> .
	Specify the AAA scheme to be applied to the domain <b>authentication default</b> { <b>hwtacacs-scheme</b> <i>hwtacacs-scheme-name</i> [ <b>local</b> ]   <b>local</b>   <b>none</b>   <b>radius-scheme</b> <i>radius-scheme-name</i> [ <b>local</b> ] }	If you specify the local AAA scheme, perform the configuration concerning local user as well. If you specify an existing scheme by providing the <i>radius-scheme-name</i> argument, perform the following configuration as well:
	Exit to system view <b>quit</b>	<ul style="list-style-type: none"> <li>For RADIUS and HWTACACS configuration, see the <i>Security Configuration Guide</i>.</li> <li>Configure the username and password on the AAA server. (For more information, see the <i>Security Configuration Guide</i>.)</li> </ul>
Create a local user and enter local user view	<b>local-user</b> <i>user-name</i>	By default, no local user exists.
Set the local password	<b>password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	Required By default, no local password is set.

To do...	Use the command...	Remarks
Specify the command level of the local user	<b>authorization-attribute level level</b>	Optional By default, the command level is 0.
Specify the service type for the local user	<b>service-type Telnet</b>	Required By default, no service type is specified.
Exit to system view	<b>quit</b>	—
Configure common settings for VTY user interfaces	—	Optional See “ <a href="#">Configuring common settings for VTY user interfaces (optional)</a> .”

After you enable command authorization, you need to perform the following configuration to make the function take effect:

- Create a HWTACACS scheme, and specify the IP address of the authorization server and other authorization parameters. For more information, see the *Security Configuration Guide*.
- Reference the created HWTACACS scheme in the ISP domain. For more information, see the *Security Configuration Guide*.

After you enable command accounting, you need to perform the following configuration to make the function take effect:

- Create a HWTACACS scheme, and specify the IP address of the accounting server and other accounting parameters. For more information, see the *Security Configuration Guide*.
- Reference the created HWTACACS scheme in the ISP domain. For more information, see the *Security Configuration Guide*.

When users adopt the scheme mode to log in to the device, the level of the commands that the users can access depends on the user privilege level defined in the AAA scheme.

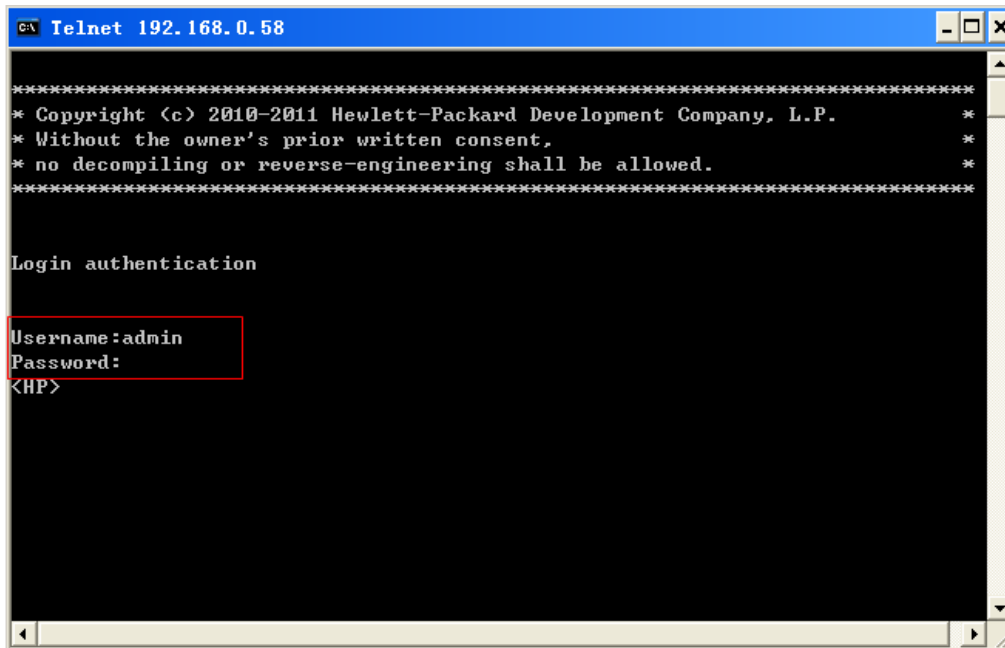
- When the AAA scheme is local, the user privilege level is defined by the **authorization-attribute level level** command.
- When the AAA scheme is RADIUS or HWTACACS, the user privilege level is configured on the RADIUS or HWTACACS server.

For more information about AAA, RADIUS, and HWTACACS, see the *Security Configuration Guide*.

When you log in to the device through Telnet again:

- You are required to enter the login username and password. A prompt such as <HP> appears after you enter the correct username (for example, admin) and password and press **Enter**, as shown in [Figure 15](#).
- After you enter the correct username and password, if the device prompts you to enter another password of the specified type, you will be authenticated for the second time. In other words, to pass authentication, you must enter a correct password as prompted.
- If “All user interfaces are used, please try later!” is displayed, it means the current login users exceed the maximum number. Please try later.

Figure 15 Configuration page



## Configuring common settings for VTY user interfaces (optional)

Follow these steps to configure common settings for VTY user interfaces:

To do...	Use the command...	Remarks	
Enter system view	<b>system-view</b>	—	
Enable display of copyright information	<b>copyright-info enable</b>	Optional Enabled by default.	
Enter one or multiple VTY user interface views	<b>user-interface vty</b> <i>first-number</i> [ <i>last-number</i> ]	—	
User interface configuration	Enable the terminal service	<b>shell</b>	Optional Enabled by default.
	Enable the current user interface(s) to support either Telnet, SSH, or both of them	<b>protocol inbound</b> { <b>all</b>   <b>ssh</b>   <b>telnet</b> }	Optional By default, both protocols are supported. The configuration takes effect next time you log in.
	Define a shortcut key for terminating tasks	<b>escape-key</b> { <b>default</b>   <i>character</i> }	Optional By default, you can press <b>Ctrl+C</b> to terminate a task.
	Configure the type of terminal display	<b>terminal type</b> { <b>ansi</b>   <b>vt100</b> }	Optional By default, the terminal display type is ANSI.

To do...	Use the command...	Remarks
Set the maximum number of lines on the next screen	<b>screen-length</b> <i>screen-length</i>	Optional By default, the next screen displays 24 lines. A value of 0 disables the function.
Set the size of history command buffer	<b>history-command max-size</b> <i>value</i>	Optional By default, the buffer saves 10 history commands.
Set the idle-timeout timer	<b>idle-timeout</b> <i>minutes</i> [ <i>seconds</i> ]	Optional The default idle-timeout is 10 minutes for all user interfaces. The system automatically terminates the user's connection if no information interaction occurs between the device and the user in timeout time. Setting idle-timeout to 0 disables the timer.
Specify a command to be automatically executed when a user logs in to the current user interface	<b>auto-execute command</b> <i>command</i>	Optional By default, command auto-execution is disabled. The system automatically executes the specified command when a user logs in to the user interface, and tears down the user connection after the command is executed. If the command triggers another task, the system does not tear down the user connection until the task is completed. A Telnet command is usually specified to enable the user to automatically Telnet to the specified device.

 **CAUTION:**

- The **auto-execute command** command may disable you from configuring the system through the user interface to which the command is applied. Use it with caution.
- Before executing the **auto-execute command** command and saving the configuration (by using the **save** command), make sure that you can access the device through VTY and AUX user interfaces so that you can remove the configuration if a problem occurs.

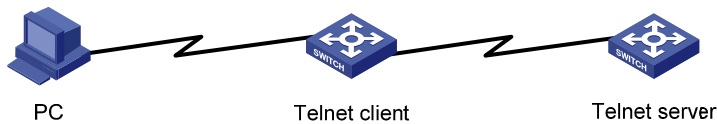
## Configuring the device to log in to a Telnet server as a Telnet client

### Configuration prerequisites

You have logged in to the device.

By default, you can log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “[Configuration requirements](#).”

**Figure 16 Log in to another device from the current device**



**NOTE:**

If the Telnet client port and the Telnet server port that connect them are not in the same subnet, make sure that the two devices can reach each other.

**Configuration procedure**

Follow the step below to configure the device to log in to a Telnet server as a Telnet client:

To do...	Use the command...	Remarks
Configure the device to log in to a Telnet server as a Telnet client	<code>telnet remote-host [ service-port ] [   [ source { interface interface-type interface-number   ip ip-address } ] ]</code>	Required Use either command
	<code>telnet ipv6 remote-host [ -i interface-type interface-number ] [ port-number ]</code>	Available in user view
Specify the source IPv4 address or source interface for sending Telnet packets	<code>telnet client source { interface interface-type interface-number   ip ip-address }</code>	Optional By, no source IPv4 address or source interface is specified. The source IPv4 address is selected by routing.

# Logging in through SSH

## Introduction

Secure Shell (SSH) offers an approach to log into a remote device securely. By providing encryption and strong authentication, it protects devices against attacks such as IP spoofing and plain text password interception. The device supports SSH, and you can log in to the device through SSH to remotely manage and maintain the device, as shown in [Figure 17](#).

**Figure 17 SSH login diagram**



The following table shows the configuration requirements of SSH login.

Object	Requirements
SSH server	Configure the IP address of the VLAN interface, and make sure the SSH server and client can reach each other.
	Configure the authentication mode and other settings.
SSH client	Run the SSH client program.
	Obtain the IP address of the VLAN interface on the server.

By default, the device is enabled with the SSH server and client functions.

- On a device that serves as the SSH client, you can log in to an SSH server to perform operations on the server.
- On a device that serves as the SSH server, you can configure the authentication mode and user level for SSH users. By default, password authentication is adopted for SSH login, but no login password is configured, so you cannot log in to the device through SSH by default. Before you can log in to the device through SSH, you need to log in to the device through the console port and configure the authentication mode, user level, and common settings.

This section includes these topics:

- [Configuring the SSH server](#)
- [Configuring the SSH client to log in to the SSH server](#)

## Configuring the SSH server

### Configuration prerequisites

You have logged in to the device, and want to log in to the device through SSH in the future.

By default, you can log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “[Configuration requirements.](#)”

### Configuration procedure

Follow these steps to configure the device that serves as an SSH server:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Create local key pair(s)	<b>public-key local create { dsa   rsa }</b>	Required By default, no local key pair(s) are created.
Enable SSH server	<b>ssh server enable</b>	Required By default, SSH server is disabled.
Enter one or more VTY user interface views	<b>user-interface vty</b> <i>first-number</i> [ <i>last-number</i> ]	—
Specify the scheme authentication mode	<b>authentication-mode scheme</b>	Required By default, authentication mode for VTY user interfaces is <b>password</b> .

To do...	Use the command...	Remarks
Enable the current user interface to support SSH	<b>protocol inbound { all   ssh }</b>	Optional By default, Telnet and SSH are supported.
Enable command authorization	<b>command authorization</b>	Optional <ul style="list-style-type: none"> <li>By default, command authorization is not enabled.</li> <li>By default, command level for a login user depends on the user privilege level. The user is authorized the command with the default level not higher than the user privilege level. With the command authorization configured, the command level for a login user is determined by both the user privilege level and AAA authorization. If a user executes a command of the corresponding command level, the authorization server checks whether the command is authorized. If yes, the command can be executed.</li> </ul>
Enable command accounting	<b>command accounting</b>	Optional <ul style="list-style-type: none"> <li>By default, command accounting is disabled. The accounting server does not record the commands executed by users.</li> <li>Command accounting allows the HWTACACS server to record all executed commands that are supported by the device, regardless of the command execution result. This helps control and monitor user operations on the device. If command accounting is enabled and command authorization is not enabled, every executed command is recorded on the HWTACACS server. If both command accounting and command authorization are enabled, only the authorized and executed commands are recorded on the HWTACACS server.</li> </ul>
Exit to system view	<b>quit</b>	—



To do...	Use the command...	Remarks
Configure the authentication mode	Enter the default ISP domain view <b>domain</b> <i>domain-name</i>	Optional By default, the AAA scheme is local.
	Apply the specified AAA scheme to the domain <b>authentication default</b> { <b>hwtacacs-scheme</b> <i>hwtacacs-scheme-name</i> [ <b>local</b> ]   <b>local</b>   <b>none</b>   <b>radius-scheme</b> <i>radius-scheme-name</i> [ <b>local</b> ] }	If you specify the local AAA scheme, perform the configuration concerning local user as well. If you specify an existing scheme by providing the <i>radius-scheme-name</i> argument, perform the following configuration as well: <ul style="list-style-type: none"> <li>For RADIUS and HWTACACS configuration, see the <i>Security Configuration Guide</i>.</li> <li>Configure the username and password on the AAA server. (For more information, see the <i>Security Configuration Guide</i>.)</li> </ul>
	Exit to system view <b>quit</b>	
Create a local user and enter local user view <b>local-user</b> <i>user-name</i>	Required By default, no local user exists.	
Set the local password <b>password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	Required By default, no local password is set.	
Specify the command level of the local user <b>authorization-attribute level</b> <i>level</i>	Optional By default, the command level is 0.	
Specify the service type for the local user <b>service-type</b> <i>ssh</i>	Required By default, no service type is specified.	
Return to system view <b>quit</b>	—	
Create an SSH user, and specify the authentication mode for the SSH user <b>ssh user</b> <i>username</i> <b>service-type</b> <b>stelnet authentication-type</b> { <b>password</b>   { <b>any</b>   <b>password-publickey</b>   <b>publickey</b> } <b>assign publickey</b> <i>keyname</i> }	Required By default, no SSH user exists, and no authentication mode is specified.	
Configure common settings for VTY user interfaces —	Optional See “ <a href="#">Configuring common settings for VTY user interfaces (optional)</a> .”	

**NOTE:**

This chapter describes how to configure an SSH client by using **password** authentication. For more information about SSH and how to configure an SSH client by using **publickey**, see the *Security Configuration Guide*.

After you enable command authorization or command accounting, you need to perform the following configuration to make the function take effect:

- Create a HWTACACS scheme, and specify the IP address of the authorization server and other authorization parameters.

- Reference the created HWTACACS scheme in the ISP domain.

For more information, see the *Security Configuration Guide*.

When users adopt the scheme mode to log in to the device, the level of the commands that the users can access depends on the user privilege level defined in the AAA scheme.

- When the AAA scheme is local, the user privilege level is defined by the **authorization-attribute level level** *level* command.
- When the AAA scheme is RADIUS or HWTACACS, the user privilege level is configured on the RADIUS or HWTACACS server.
- For more information about AAA, RADIUS, and HWTACACS, see the *Security Configuration Guide*.

## Configuring the SSH client to log in to the SSH server

### Configuration prerequisites

You have logged in to the device.

By default, you can log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “[Configuration requirements](#).”

**Figure 18 Log in to another device from the current device**



#### NOTE:

If the SSH client and the SSH server are not in the same subnet, make sure that the two devices can reach each other.

### Configuration procedure

Follow these steps to configure the SSH client to log in to the SSH server:

To do...	Use the command...	Remarks
Log in to an IPv4 SSH server	<b>ssh2 server</b>	Required server is the IPv4 address or host name of the server. Available in user view
Log in to an IPv6 SSH server	<b>ssh2 ipv6 server</b>	Required server is the IPv6 address or host name of the server. Available in user view

#### NOTE:

You can configure other settings for the SSH client to work with the SSH server. For more information, see the *Security Configuration Guide*.

# Logging in through modems

## Introduction

The administrator can use two modems to remotely maintain a switch through its Console port over the Public Switched Telephone Network (PSTN) when the IP network connection is broken.

This section includes these topics:

- [Configuration requirements](#)
- [Login procedure](#)
- [Modem login authentication modes](#)
- [Configuring none authentication for modem login](#)
- [Configuring password authentication for modem login](#)
- [Configuring scheme authentication for modem login](#)
- [Configuring common settings for modem login \(optional\)](#)

## Configuration requirements

By default, no authentication is needed when you log in through modems, and the default user privilege level is 3.

To use this method, perform necessary configurations on both the device side and administrator side.

The following table shows the remote login configuration requirements through the console port by using modem dial-in:

Object	Requirement
Administrator side	The PC is correctly connected to the modem.
	The modem is connected to a telephone cable that works properly.
	The telephone number of the remote modem connected to the console port of the remote switch is obtained.
Device side	The console port is correctly connected to the modem.
	Configurations have been configured on the modem.
	The modem is connected to a telephone cable that works properly.
	Authentication configuration has been completed on the remote switch.

## Login procedure

- Step1** Set up a configuration environment as shown in [Figure 19](#): connect the serial port of the PC and the console port of the device to a modem respectively.

**Figure 19** Set up a configuration terminal



**Step2** Configuration on the administrator side

The PC and the modem are correctly connected, the modem is connected to a telephone cable, and the telephone number of the remote modem connected to the console port of the remote switch is obtained.

---

**NOTE:**

Note the following device settings:

- The baud rate of the Console port is lower than the transmission rate of the modem. Otherwise, packets may be lost.
  - The parity check mode, stop bits, and data bits of the console port adopt the default settings.
- 

**Step3** Perform the following configurations on the modem that is directly connected to the device:

```
AT&F          ----- Restore the factory defaults
ATS0=1       ----- Configure auto-answer on first ring
AT&D         ----- Ignore data Terminal Ready signals
AT&K0        ----- Disable local flow control
AT&R1        ----- Ignore Data Flow Control signals
AT&S0        ----- Force DSR to remain on
ATEQ1&W     ----- Disable the modem from response to commands and save the
configuration
```

To verify your configuration, enter AT&V to show the configuration results.

---

**NOTE:**

The configuration commands and the output for different modems may be different. For more information, see your modem's user guide.

---

**Step4** Launch a terminal emulation utility (such as HyperTerminal in Windows XP/Windows 2000), and create a new connection (the telephone number is the number of the modem connected to the device).

---

**NOTE:**

On Windows 2003 Server operating system, you need to add the HyperTerminal program first, and then log in to and manage the device as described in this document. On Windows 2008 Server, Windows 7, Windows Vista, or some other operating system, you need to obtain a third party terminal control program first, and follow that program's user guide or online help to log in to the device.

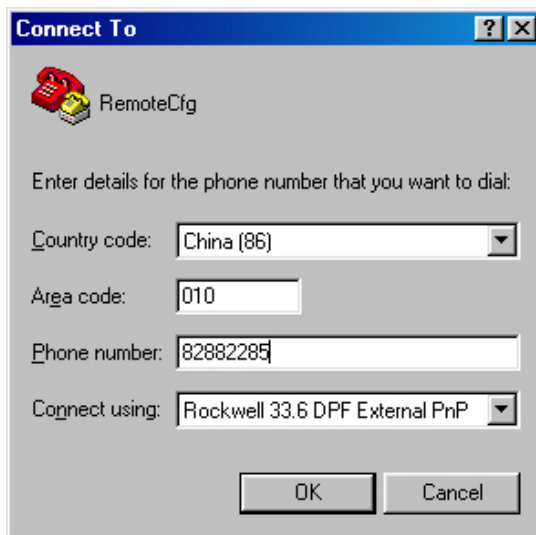
---

**Step5** Dial the destination number on the PC to establish a connection with the device, as shown in [Figure 20](#) through [Figure 22](#).

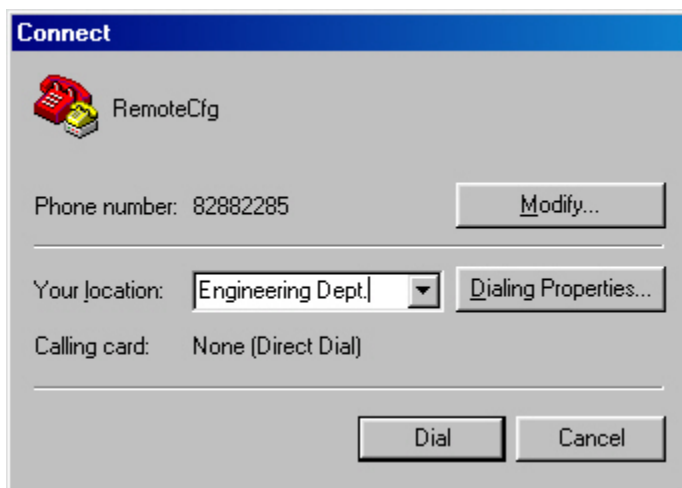
**Figure 20 Connection description**



**Figure 21 Enter the phone number**

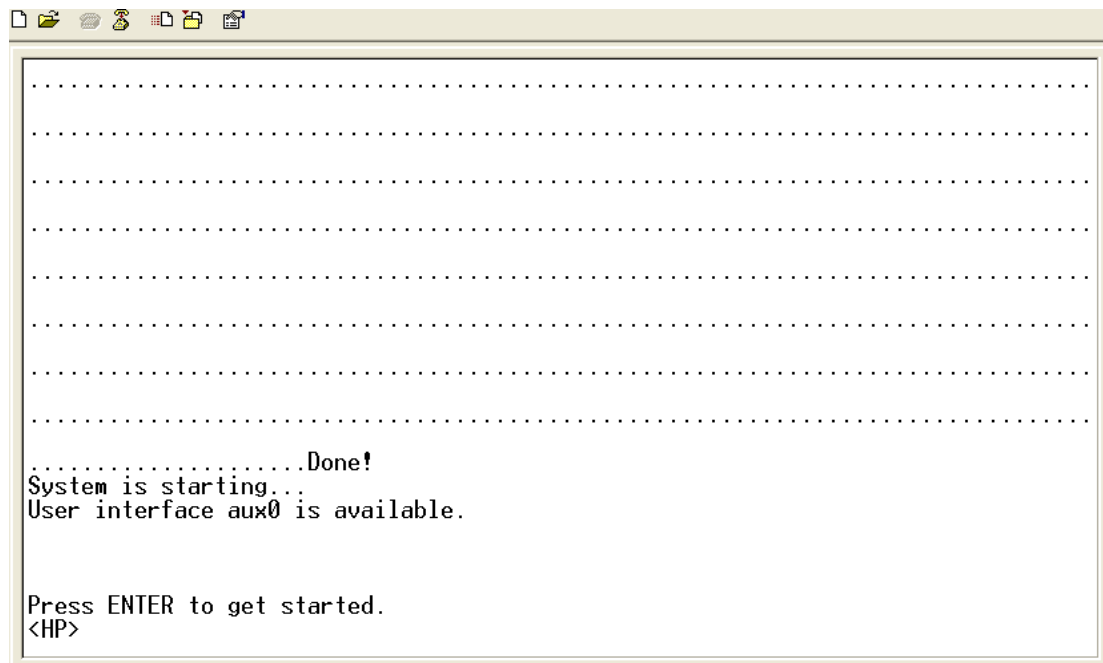


**Figure 22 Dial the number**



**Step6** Character string CONNECT9600 is displayed on the terminal. Then a prompt appears when you press **Enter**.


**Figure 23 Configuration page**



**Step7** If the authentication mode is **password**, a prompt (for example, HP) appears when you type the configured password on the remote terminal. Then you can configure or manage the router. To get help, type **?**.

**Step8** Execute commands to configure the device or check the running status of the device. To get help, type **?**.

**NOTE:**

- To terminate the connection between the PC and device, execute the **ATH** command on the terminal to terminate the connection between the PC and modem. If you cannot execute the command on the terminal, input AT+ + + and then press **Enter**. When you are prompted **OK**, execute the **ATH** command, and the connection is terminated if **OK** is displayed. You can also terminate the connection between the PC and device by clicking  on the hyper terminal window.
- Do not close the hyper terminal directly. Otherwise, the remote modem may always be online, and you will fail to dial in the next time.

## Modem login authentication modes

The following authentication modes are available for modem dial-in login: **none**, **password**, and **scheme**.

- **none**—Requires no username and password at the next login through modems. This mode is insecure.
- **password**—Requires password authentication at the next login through the console port. Keep your password.
- **scheme**—Requires username and password authentication at the next login through the console port. Authentication falls into local authentication and remote authentication. To use local authentication, configure a local user and related parameters. To use remote authentication, configure the username

and password on the remote authentication server. For more information about authentication modes and parameters, see the *Security Configuration Guide*. Keep your username and password.

The following table lists modem login configurations for different authentication modes:

Authentication mode	Configuration	Remarks	
None	Configure not to authenticate users	For more information, see <a href="#">“Configuring none authentication for modem login.”</a>	
Password	Configure to authenticate users by using the local password	For more information, see <a href="#">“Configuring password authentication for modem login.”</a>	
	Set the local password		
Scheme	Configure the authentication scheme	For more information, see <a href="#">“Configuring scheme authentication for modem login.”</a>	
	Remote AAA authentication		Configure a RADIUS/HWTACACS scheme
			Configure the AAA scheme used by the domain
	Select an authentication scheme		Configure the username and password on the AAA server
	Local authentication	Configure the authentication username and password	
		Configure the AAA scheme used by the domain as local	

**NOTE:**

Modem login authentication changes do not take effect until you exit the CLI and log in again.

## Configuring none authentication for modem login

### Configuration prerequisites

You have logged in to the device.

By default, you can log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see [“Configuration requirements.”](#)

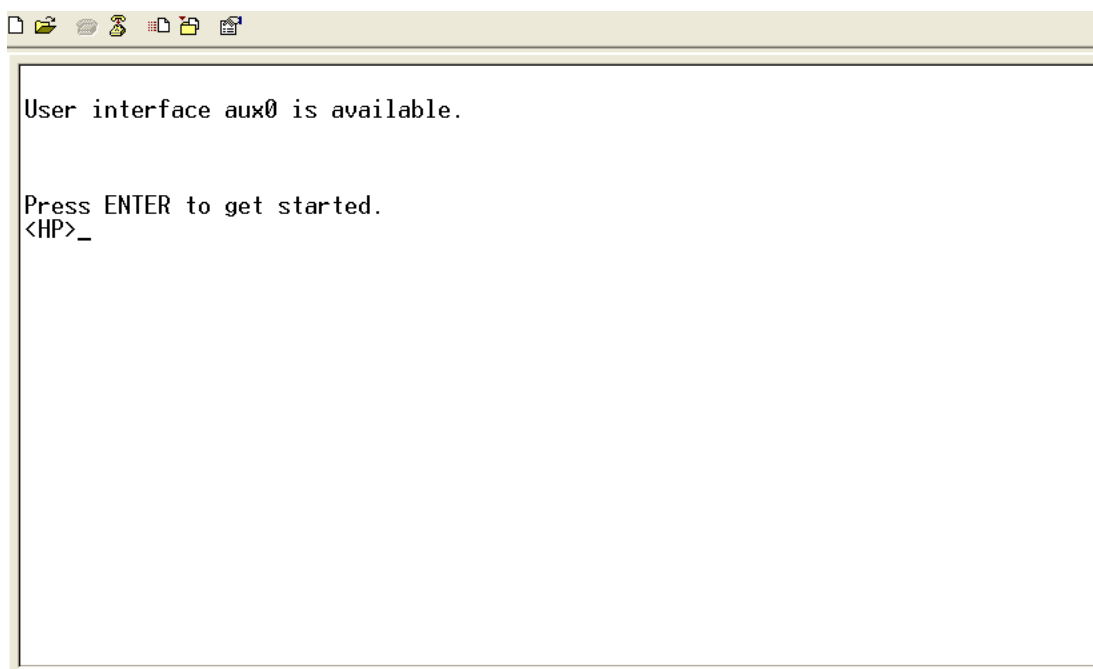
### Configuration procedure

Follow these steps to configure none authentication for modem login:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enter one or more AUX user interface views	<b>user-interface aux</b> <i>first-number</i> [ <i>last-number</i> ]	—
Specify the none authentication mode	<b>authentication-mode none</b>	Required By default, users that log in through the console port are not authenticated.
Configure common settings for VTY user interfaces	—	Optional See " <a href="#">Configuring common settings for VTY user interfaces (optional)</a> ."

When you log in to the device through modems after the configuration, you are prompted to press **Enter**. A prompt such as <HP> appears after you press **Enter**, as shown in [Figure 24](#).

**Figure 24 Configuration page**



## Configuring password authentication for modem login

### Configuration prerequisites

You have logged in to the device.

By default, you can log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see "[Configuration requirements](#)."

### Configuration procedure

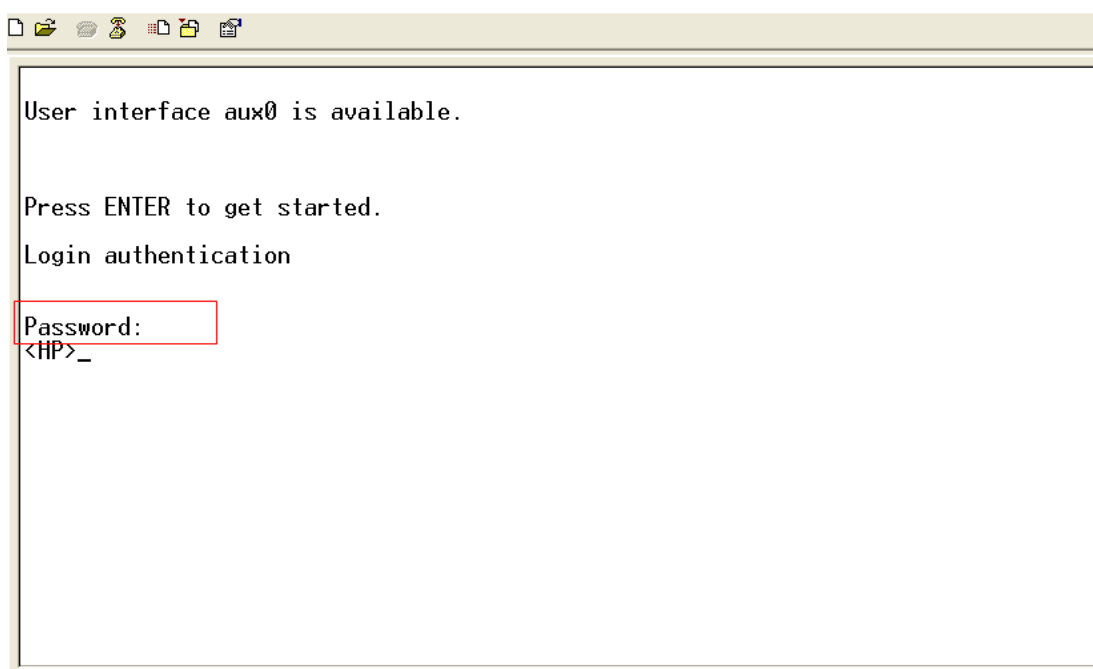
Follow these steps to configure password authentication for modem login:



To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enter one or more AUX user interface views	<b>user-interface aux</b> <i>first-number</i> [ <i>last-number</i> ]	—
Specify the password authentication mode	<b>authentication-mode password</b>	Required By default, the authentication mode is none for modem users
Set the local password	<b>set authentication password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	Required By default, no local password is set.
Configure common settings for VTY user interfaces	—	Optional For more information, see <a href="#">“Configuring common settings for VTY user interfaces (optional).”</a>

When you log in to the device through modems after the configuration, you are prompted to enter a login password. A prompt such as <HP> appears after you input the password and press **Enter**, as shown in [Figure 25](#).

**Figure 25 Configuration page**



## Configuring scheme authentication for modem login

### Configuration prerequisites

You have logged in to the device.

By default, you can log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see [“Configuration requirements.”](#)

## Configuration procedure

Follow these steps to configure scheme authentication for modem login:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enter AUX user interface view	<b>user-interface aux</b> <i>first-number</i> [ <i>last-number</i> ]	—
Specify the scheme authentication mode	<b>authentication-mode scheme</b>	<p>Required</p> <p>Whether local, RADIUS, or HWTACACS authentication is adopted depends on the configured AAA scheme.</p> <p>By default, the authentication mode is none for modem users</p>
Enable command authorization	<b>command authorization</b>	<p>Optional</p> <ul style="list-style-type: none"> <li>• By default, command authorization is not enabled.</li> <li>• By default, command level for a login user depends on the user privilege level. The user is authorized the command with the default level not higher than the user privilege level. With the command authorization configured, the command level for a login user is determined by both the user privilege level and AAA authorization. If a user executes a command of the corresponding command level, the authorization server checks whether the command is authorized. If yes, the command can be executed.</li> <li>• Before enabling command authorization, configure the AAA authorization server. After you enable command authorization, only commands authorized by the AAA authorization server can be executed.</li> </ul>

To do...	Use the command...	Remarks	
Enable command accounting	<b>command accounting</b>	<p>Optional</p> <ul style="list-style-type: none"> <li>By default, command accounting is disabled. The accounting server does not record the commands executed by users.</li> <li>Command accounting allows the HWTACACS server to record all executed commands that are supported by the device, regardless of the command execution result. This helps control and monitor user operations on the device. If command accounting is enabled and command authorization is not enabled, every executed command is recorded on the HWTACACS server. If both command accounting and command authorization are enabled, only the authorized and executed commands are recorded on the HWTACACS server.</li> <li>Configure the AAA accounting server before enabling command accounting.</li> </ul>	
Exit to system view	<b>quit</b>	—	
Configure the authentication mode	Enter the default ISP domain view	<b>domain</b> <i>domain-name</i>	<p>Optional</p> <p>By default, the AAA scheme is <b>local</b>.</p> <p>If you specify the local AAA scheme, perform the configuration concerning local user as well. If you specify an existing scheme by providing the <i>radius-scheme-name</i> argument, perform the following configuration as well:</p> <ul style="list-style-type: none"> <li>For RADIUS and HWTACACS configuration, see the <i>Security Configuration Guide</i>.</li> <li>Configure the username and password on the AAA server. (For more information, see the <i>Security Configuration Guide</i>.)</li> </ul>
	Apply the specified AAA scheme to the domain	<b>authentication default</b> { <b>hwtacacs-scheme</b> <i>hwtacacs-scheme-name</i> [ <b>local</b> ]   <b>local</b>   <b>none</b>   <b>radius-scheme</b> <i>radius-scheme-name</i> [ <b>local</b> ] }	
	Return to system view	<b>quit</b>	
Create a local user and enter local user view	<b>local-user</b> <i>user-name</i>	<p>Required</p> <p>By default, no local user exists.</p>	
Set the authentication password for the local user	<b>password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	Required	
Specify the command level of the local user	<b>authorization-attribute level</b> <i>level</i>	<p>Optional</p> <p>By default, the command level is 0.</p>	

To do...	Use the command...	Remarks
Specify the service type for the local user	<b>service-type terminal</b>	Required By default, no service type is specified.
Configure common settings for VTY user interfaces	—	Optional See <a href="#">“Configuring common settings for VTY user interfaces (optional).”</a>

After you enable command authorization, you need to perform the following configuration to make the function take effect:

- Create a HWTACACS scheme, and specify the IP address of the authorization server and other authorization parameters. For more information, see the *Security Configuration Guide*.
- Reference the created HWTACACS scheme in the ISP domain. For more information, see the *Security Configuration Guide*.

After you enable command accounting, you need to perform the following configuration to make the function take effect:

- Create a HWTACACS scheme, and specify the IP address of the accounting server and other accounting parameters. For more information, see the *Security Configuration Guide*.
- Reference the created HWTACACS scheme in the ISP domain. For more information, see the *Security Configuration Guide*.

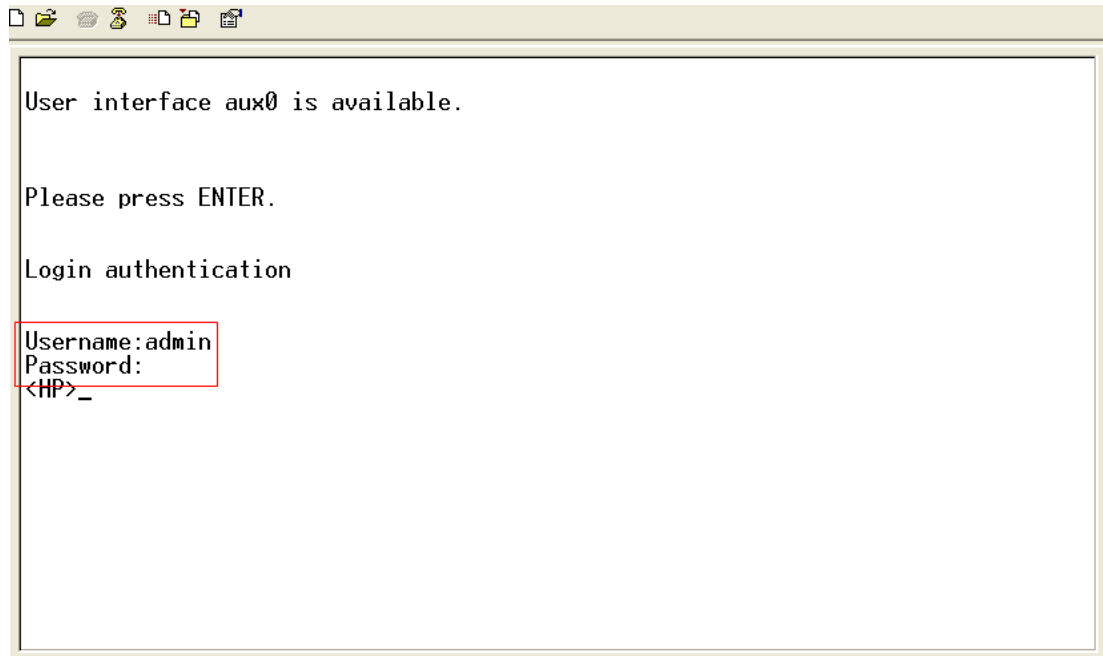
When users adopt the scheme mode to log in to the device, the level of the commands that the users can access depends on the user privilege level defined in the AAA scheme.

- When the AAA scheme is local, the user privilege level is defined by the **authorization-attribute level level** command.
- When the AAA scheme is RADIUS or HWTACACS, the user privilege level is configured on the RADIUS or HWTACACS server.

For more information about AAA, RADIUS, and HWTACACS, see the *Security Configuration Guide*.

When you log in to the device through modems after the configuration, you are prompted to enter a login username and password. A prompt such as <HP> appears after you input the password and username and press **Enter**, as shown in [Figure 26](#).

Figure 26 Configuration page



## Configuring common settings for modem login (optional)

Follow these steps to configure common settings for modem login:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enable display of copyright information	<b>copyright-info enable</b>	Optional Enabled by default.
Enter one or more AUX user interface views	<b>user-interface aux</b> <i>first-number</i> [ <i>last-number</i> ]	—
Configure AUX user interface properties	Configure the baud rate	Optional By default ,the baud rate is 9600 bps. Transmission rate is the number of bits that the device transmits to the terminal per second.
	Configure the parity check mode	Optional By default, the parity check mode is <b>none</b> , which means no check bit.
	Configure the stop bits	Optional By default, the stop bits of the console port is 1. Stop bits are the last bits transmitted in data transmission to unequivocally indicate the end of a character. The more the bits are, the slower the transmission is.

To do...	Use the command...	Remarks
Configure the data bits	<b> databits { 5   6   7   8 }</b>	Optional By default, the data bits is 8. Data bits is the number of bits representing one character. The setting depends on the contexts to be transmitted. For example, you can set it to 7 if standard ASCII characters are to be sent, and set it to 8 if extended ASCII characters are to be sent.
Define a shortcut key for starting a session	<b> activation-key </b> <i>character</i>	Optional By default, you can press <b>Enter</b> to start a session.
Define a shortcut key for terminating tasks	<b> escape-key { default   character }</b>	Optional By default, you can press <b>Ctrl+C</b> to terminate a task.
Configure the flow control mode	<b> flow-control { hardware   none   software }</b>	Optional By default, the value is <b>none</b>
Configure the type of terminal display	<b> terminal type { ansi   vt100 }</b>	Optional By default, the terminal display type is ANSI. The device supports two types of terminal display: ANSI and VT100. HP recommends that you set the display type of both the device and the client to VT100. If the device and the client use different display types (for example, hyper terminal or Telnet terminal) or both are set to ANSI, when the total number of characters of the edited command line exceeds 80, an anomaly such as cursor corruption or abnormal display of the terminal display may occur on the client.
Configure the user privilege level for login users	<b> user privilege level </b> <i>level</i>	Optional 3 by default.
Set the maximum number of lines on the next screen	<b> screen-length </b> <i>screen-length</i>	Optional By default, the next screen displays 24 lines at most. A value of 0 disables the function.
Set the size of the history command buffer	<b> history-command max-size </b> <i>value</i>	Optional By default, the buffer saves 10 history commands at most.

To do...	Use the command...	Remarks
Set the idle-timeout timer	<b>idle-timeout</b> <i>minutes</i> [ <i>seconds</i> ]	Optional The default idle-timeout is 10 minutes. The system automatically terminates the user's connection if no information interaction occurs between the device and the user within the idle-timeout time. Setting idle-timeout to 0 disables the timer.

**CAUTION:**

- The common settings configured for console login take effect immediately. If you configure the common settings after you log in through the console port, the current connection may be interrupted. To avoid this problem, use another login method. After you configure the common settings for console login, you will need to modify the settings on the terminal to make them consistent with those on the device.
- The baud rate of the console port must be lower than the transmission rate of the modem. Otherwise, packets may be lost.

## Displaying and maintaining CLI login

To do...	Use the command...	Remarks
Display the source IP address/interface specified for Telnet packets	<b>display telnet client configuration</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display information about the user interfaces that are being used	<b>display users</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Displays information about all user interfaces that the device supports	<b>display users all</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display user interface information	<b>display user-interface</b> [ <i>num1</i>   { <b>aux</b>   <b>vty</b> } <i>num2</i> ] [ <b>summary</b> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view

To do...	Use the command...	Remarks
Release a specified user interface	<b>free user-interface</b> { <i>num1</i>   { <b>aux</b>   <b>vty</b> } <i>num2</i> }	<p>Available in user view</p> <p>Multiple users can log in to the system to simultaneously configure the device. In some circumstances, when the administrator wants to make configurations without interruption from the users that have logged in through other user interfaces, the administrator can execute the command to release the connections established on the specified user interfaces.</p> <p>You cannot use this command to release the connection that you are using.</p>
Lock the current user interface	<b>lock</b>	<p>Available in user view</p> <p>By default, the current user interface is not locked.</p>
Send messages to the specified user interfaces	<b>send</b> { <b>all</b>   <i>num1</i>   { <b>aux</b>   <b>vty</b> } <i>num2</i> }	Available in user view



# Web login

## Web login overview

The device provides a built-in web server that enables you to log in to the web interface of the device from a PC. Web login is disabled by default.

To enable web login, log in to the device via the console port, and perform the following configuration:

- Enable HTTP or HTTPS service
- Configure the IP address of the VLAN interface
- Configure a username and password

The device supports the following web login methods:

- HTTP login: The Hypertext Transfer Protocol (HTTP) is used for transferring web page information across the Internet. It is an application-layer protocol in the TCP/IP protocol suite. The connection-oriented Transport Control Protocol (TCP) is adopted at the transport layer. The device supports HTTP 1.0.
- HTTPS login: The Secure HTTP (HTTPS) refers to the HTTP protocol that supports the Security Socket Layer (SSL) protocol. HTTPS uses SSL to encrypt the data exchanged between the HTTPS client and the server to ensure data security and integrity. You can define a certificate attribute-based access control policy to allow legal clients to access the device securely and to prohibit illegal clients.

The following table shows the configuration requirements of web login.

Object	Requirements
Device	Configure the IP address of the VLAN interface
	Make sure the device and the PC can reach each other
	<a href="#">Configuring HTTP login</a> — Required to use one approach
	<a href="#">Configuring HTTPS login</a>
PC	Install a web browser
	Obtain the IP address of the VLAN interface of the device

## Configuring HTTP login

Follow these steps to configure HTTP login:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enable the HTTP service	<b>ip http enable</b>	Required Enabled by default.

To do...	Use the command...	Remarks
Configure the HTTP service port number	<b>ip http port</b> <i>port-number</i>	Optional 80 by default. If you execute the command multiple times, the last one takes effect.
Associate the HTTP service with an ACL	<b>ip http acl</b> <i>acl-number</i>	Optional By default, the HTTP service is not associated with any ACL. Associating the HTTP service with an ACL enables the device to allow only clients permitted by the ACL to access the device.
Create a local user and enter local user view	<b>local-user</b> <i>user-name</i>	Required By default, no local user is configured.
Configure a password for the local user	<b>password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	Required By default, no password is configured for the local user.
Specify the command level of the local user	<b>authorization-attribute level</b> <i>level</i>	Required No command level is configured for the local user.
Specify the Telnet service type for the local user	<b>service-type telnet</b>	Required By default, no service type is configured for the local user.
Exit to system view	<b>quit</b>	—
Create a VLAN interface and enter its view	<b>interface vlan-interface</b> <i>vlan-interface-id</i>	Required If the VLAN interface already exists, the command enters its view.
Assign an IP address and subnet mask to the VLAN interface	<b>ip address</b> <i>ip-address</i> { <i>mask</i>   <i>mask-length</i> }	Required By default, no IP address is assigned to the VLAN interface.

## Configuring HTTPS login

Follow these steps to configure HTTPS login:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—

To do...	Use the command...	Remarks
Configure PKI and SSL related features	—	<p>Required</p> <p>By default, PKI and SSL are not configured.</p> <ul style="list-style-type: none"> <li>• For more information about PKI, see the <i>Security Configuration Guide</i>.</li> <li>• For more information about SSL, see the <i>Security Configuration Guide</i>.</li> </ul>
Associate the HTTPS service with an SSL server policy	<b>ip https ssl-server-policy</b> <i>policy-name</i>	<p>Required</p> <p>By default, the HTTPS service is not associated with any SSL server policy.</p> <ul style="list-style-type: none"> <li>• If you disable the HTTPS service, the system automatically de-associates the HTTPS service from the SSL service policy. Before re-enabling the HTTPS service, associate the HTTPS service with an SSL server policy first.</li> <li>• Any changes to the SSL server policy associated with the HTTP service that is enabled do not take effect.</li> </ul>
Enable the HTTPS service	<b>ip https enable</b>	<p>Required</p> <p>Disabled by default.</p> <p>Enabling the HTTPS service triggers an SSL handshake negotiation process. During the process, if the local certificate of the device exists, the SSL negotiation succeeds, and the HTTPS service can be started normally. If no local certificate exists, a certificate application process will be triggered by the SSL negotiation. Because the application process takes much time, the SSL negotiation often fails and the HTTPS service cannot be started normally. In that case, you need to execute the <b>ip https enable</b> command multiple times to start the HTTPS service.</p>

To do...	Use the command...	Remarks
Associate the HTTPS service with a certificate attribute-based access control policy	<b>ip https certificate access-control-policy</b> <i>policy-name</i>	Optional By default, the HTTPS service is not associated with any certificate-based attribute access control policy. <ul style="list-style-type: none"> <li>• Associating the HTTPS service with a certificate-based attribute access control policy enables the device to control the access rights of clients.</li> <li>• You must configure the <b>client-verify enable</b> command in the associated SSL server policy. If not, no clients can log in to the device.</li> <li>• The associated SSL server policy must contain at least one <b>permit</b> rule. Otherwise, no clients can log in to the device.</li> <li>• For more information about certificate attribute-based access control policies, see the <i>Security Configuration Guide</i>.</li> </ul>
Configure the port number of the HTTPS service	<b>ip https port</b> <i>port-number</i>	Optional 443 by default.
Associate the HTTPS service with an ACL	<b>ip https acl</b> <i>acl-number</i>	Required By default, the HTTPS service is not associated with any ACL. Associating the HTTPS service with an ACL enables the device to allow only clients permitted by the ACL to access the device.
Create a local user and enter local user view	<b>local-user</b> <i>user-name</i>	Required By default, no local user is configured.
Configure a password for the local user	<b>password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	Required By default, no password is configured for the local user.
Specify the command level of the local user	<b>authorization-attribute level</b> <i>level</i>	Required By default, no command level is configured for the local user.
Specify the Telnet service type for the local user	<b>service-type telnet</b>	Required By default, no service type is configured for the local user.
Exit to system view	<b>quit</b>	—
Create a VLAN interface and enter its view	<b>interface vlan-interface</b> <i>vlan-interface-id</i>	Required If the VLAN interface already exists, the command enters its view.
Assign an IP address and subnet mask to the VLAN interface	<b>ip address</b> <i>ip-address</i> { <i>mask</i>   <i>mask-length</i> }	Required By default, no IP address is assigned to the VLAN interface.

# Displaying and maintaining web login

To do...	Use the command...	Remarks
Display information about web users	<b>display web users</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display HTTP state information	<b>display ip http</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display HTTPS state information	<b>display ip https</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view

## Web login example

### HTTP login example

#### Network requirements

As shown in [Figure 27](#), the PC is connected to the device over an IP network. The IP address of the Device is 192.168.20.66/24.

**Figure 27 Network diagram for configuring HTTP login**



#### Configuration procedure

##### 1. Configuration on the device

# Log in to the device via the console port and configure the IP address of VLAN 1 of the device. VLAN 1 is the default VLAN.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-VLAN-interfacel] ip address 192.168.20.66 255.255.255.0
[Sysname-VLAN-interfacel] quit
```

# Create a local user named **admin**, and set the password to **admin** for the user. Specify the Telnet service type for the local user, and set the command level to 3 for this user.

```
[Sysname] local-user admin
[Sysname-luser-admin] service-type telnet
[Sysname-luser-admin] authorization-attribute level 3
[Sysname-luser-admin] password simple admin
```

##### 2. Configuration on the PC

# On the PC, run the web browser. Enter the IP address of the device in the address bar, 192.168.20.66 in this example. The web login page appears, as shown in [Figure 28](#).

Figure 28 Web login page



# Type the user name, password, verify code, select **English**, and click **Login**. The homepage appears. After login, you can configure device settings through the web interface.

## HTTPS login example

### Network requirements

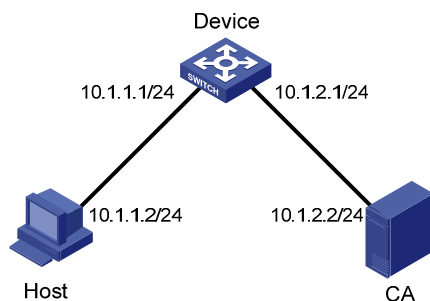
As shown in Figure 29, to prevent unauthorized users from accessing the Device, configure HTTPS login as follows:

- Configure the Device as the HTTPS server, and request a certificate for it.
- The Host acts as the HTTPS client. Request a certificate for it.

In this example, Windows Server acts as the CA. Install Simple Certificate Enrollment Protocol (SCEP) add-on on the CA. The name of the CA that issues certificates to the Device and Host is new-ca.

Before performing the following configuration, make sure that the Device, Host, and CA can reach each other.

Figure 29 Network diagram for configuring HTTPS login



## Configuration procedure

1. Configure the device that acts as the HTTPS server

# Configure a PKI entity, configure the common name of the entity as **http-server1**, and the FQDN of the entity as **ssl.security.com**.

```
<Device> system-view
[Device] pki entity en
[Device-pki-entity-en] common-name http-server1
[Device-pki-entity-en] fqdn ssl.security.com
[Device-pki-entity-en] quit
```

# Create a PKI domain, specify the trusted CA as **new-ca**, the URL of the server for certificate request as **http://10.1.2.2/certsrv/mscep/mscep.dll**, authority for certificate request as **RA**, and the entity for certificate request as **en**.

```
[Device] pki domain 1
[Device-pki-domain-1] ca identifier new-ca
[Device-pki-domain-1] certificate request url http://10.1.2.2/certsrv/mscep/mscep.dll
[Device-pki-domain-1] certificate request from ra
[Device-pki-domain-1] certificate request entity en
[Device-pki-domain-1] quit
```

# Create RSA local key pairs.

```
[Device] public-key local create rsa
```

# Retrieve the CA certificate from the certificate issuing server.

```
[Device] pki retrieval-certificate ca domain 1
```

# Request a local certificate from a CA through SCEP for the device.

```
[Device] pki request-certificate domain 1
```

# Create an SSL server policy **myssl**, specify PKI domain 1 for the SSL server policy, and enable certificate-based SSL client authentication.

```
[Device] ssl server-policy myssl
[Device-ssl-server-policy-myssl] pki-domain 1
[Device-ssl-server-policy-myssl] client-verify enable
[Device-ssl-server-policy-myssl] quit
```

# Create a certificate attribute group **mygroup1**, and configure a certificate attribute rule, specifying that the Distinguished Name (DN) in the subject name includes the string of new-ca.

```
[Device] pki certificate attribute-group mygroup1
[Device-pki-cert-attribute-group-mygroup1] attribute 1 issuer-name dn ctn new-ca
[Device-pki-cert-attribute-group-mygroup1] quit
```

# Create a certificate attribute-based access control policy **myacp**. Configure a certificate attribute-based access control rule, specifying that a certificate is considered valid when it matches an attribute rule in certificate attribute group **myacp**.

```
[Device] pki certificate access-control-policy myacp
[Device-pki-cert-acp-myacp] rule 1 permit mygroup1
[Device-pki-cert-acp-myacp] quit
```

# Associate the HTTPS service with SSL server policy **myssl**.

```
[Device] ip https ssl-server-policy myssl
```

# Associate the HTTPS service with certificate attribute-based access control policy **myacp**.

```
[Device] ip https certificate access-control-policy myacp
```

# Enable the HTTPS service.

```
[Device] ip https enable
```

# Create a local user named **usera**, set the password to **123** for the user, and specify the Telnet service type for the local user.

```
[Device] local-user usera
```

```
[Device-luser-usera] password simple 123
```

```
[Device-luser-usera] service-type telnet
```

## 2. Configure the host that acts as the HTTPS client

On the host, run the IE browser. In the address bar, enter **http://10.1.2.2/certsrv** and request a certificate for the host as prompted.

## 3. Verify the configuration

Enter **https://10.1.1.1** in the address bar, and select the certificate issued by **new-ca**. Then the web login page of the Device appears. On the login page, type the username **usera**, and password **123** to enter the web management page.

---

### NOTE:

- To log in to the web interface through HTTPS, enter the URL address starting with **https://**. To log in to the web interface through HTTP, enter the URL address starting with **http://**.
  - For more information about PKI configuration commands, see the *Security Command Reference*.
  - For more information about the public-key local create rsa command, see the *Security Command Reference*.
  - For more information about SSL configuration commands, see the *Security Command Reference*.
-



# NMS login

## NMS login overview

An NMS runs the SNMP client software. It offers a user-friendly interface to facilitate network management. An agent is a program that resides in the device. It receives and handles requests from the NMS. An NMS is a manager in an SNMP enabled network, whereas agents are managed by the NMS. The NMS and agents exchange information through the SNMP protocol. The device supports multiple NMS programs, such as iMC and CAMS.

By default, you cannot log in to the device through NMS. To enable NMS login, log in to the device via the console port and make the configuration changes described in the following table.

The following table shows the configuration requirements of NMS login.

Object	Requirements
Device	Configure the IP address of the VLAN interface
	Make sure the device and the NMS can reach each other
NMS	Configure SNMP settings
	Configure the NMS. For more information, see your NMS manual.

## Configuring NMS login

Connect the Ethernet port of the PC to an Ethernet port of VLAN 1 of the device, as shown in [Figure 30](#). Make sure the PC and VLAN 1 interface can reach each other.

**Figure 30 Network diagram for configuring NMS login**



Follow these steps to configure SNMPv3 settings:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enable SNMP agent	<b>snmp-agent</b>	Optional Disabled by default. You can enable SNMP agent with this command or any command that begins with <b>snmp-agent</b> .
Configure an SNMP group and specify its access right	<b>snmp-agent group v3</b> <i>group-name</i> [ <b>authentication</b>   <b>privacy</b> ] [ <b>read-view</b> <i>read-view</i> ] [ <b>write-view</b> <i>write-view</i> ] [ <b>notify-view</b> <i>notify-view</i> ] [ <b>acl</b> <i>acl-number</i> ]	Required By default, no SNMP group is configured.

To do...	Use the command...	Remarks
Add a user to the SNMP group	<code>snmp-agent usm-user v3 user-name group-name [ [ cipher ] authentication-mode { md5   sha } auth-password [ privacy-mode { 3des   aes128   des56 } priv-password ] ] [ acl acl-number ]</code>	Required If the <b>cipher</b> keyword is specified, both <i>auth-password</i> and <i>priv-password</i> are cipher text passwords.

Follow these steps to configure SNMPv1 and SNMPv2c settings:

To do...	Use the command...	Remarks	
Enter system view	<code>system-view</code>	—	
Enable SNMP agent	<code>snmp-agent</code>	Optional Disabled by default. You can enable SNMP agent with this command or any command that begins with <b>snmp-agent</b> .	
Create or update MIB view information	<code>snmp-agent mib-view { excluded   included } view-name oid-tree [ mask mask-value ]</code>	Optional By default, the MIB view name is ViewDefault and OID is 1.	
Configure SNMP NMS access right	Directly Configure an SNMP community	<code>snmp-agent community { read   write } community-name [ acl acl-number   mib-view view-name ]*</code>	Required Use either approach. The direction configuration approach is for SNMPv1 or SNMPv2c. The community name configured on the NMS should be consistent with the username configured on the agent.
	Indirectly Configure an SNMP group	<code>snmp-agent group { v1   v2c } group-name [ read-view read-view ] [ write-view write-view ] [ notify-view notify-view ] [ acl acl-number ]</code>	The indirect configuration approach is for SNMPv3.
	Add a user to the SNMP group	<code>snmp-agent usm-user { v1   v2c } user-name group-name [ acl acl-number ]</code>	

#### NOTE:

The device supports the following SNMP versions: SNMPv1, SNMPv2c and SNMPv3. For more information about SNMP, see the *Network Management and Monitoring Configuration Guide*.

## NMS login example

In this example, iMC is used as the NMS.

### 1. Configuration on the device

# Assign IP address of device. Make sure the device and the NMS can reach each other. (Configuration steps are omitted.)

# Enter system view.

```
<Sysname> system-view
```

# Enable the SNMP agent.

```
[Sysname] snmp-agent
```

# Configure an SNMP group.

```
[Sysname] snmp-agent group v3 managev3group read-view test write-view test
```

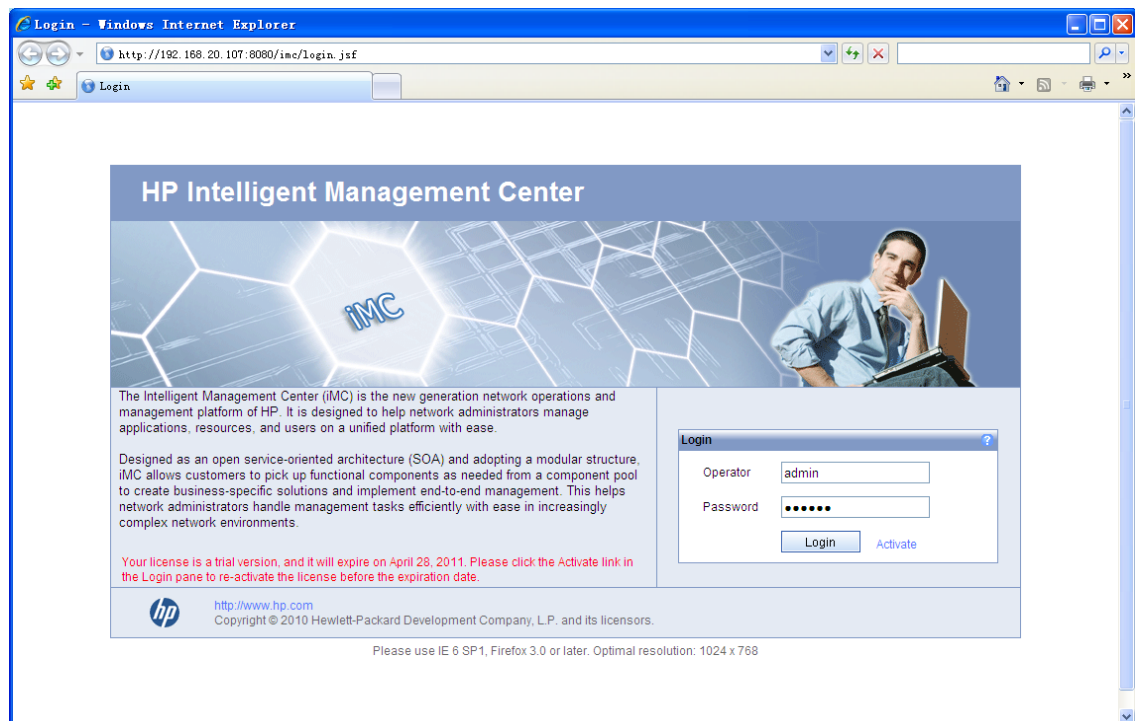
# Add a user to the SNMP group.

```
[Sysname] snmp-agent usm-user v3 managev3user managev3group
```

## 2. Configuration on the NMS

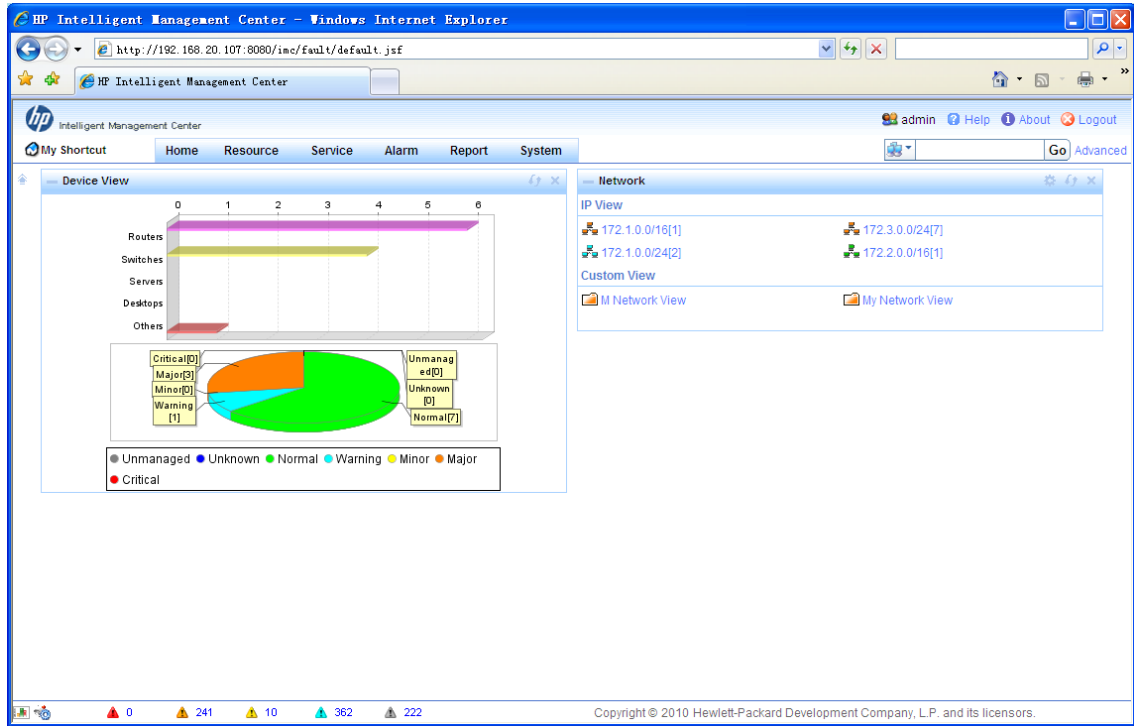
On the PC, start the browser. In the address bar, enter **http://192.168.20.107:8080/imc**, where 192.168.20.107 is the IP address of the iMC.

**Figure 31** iMC login page



Type the username and password, and then click **Login**. The iMC homepage appears, as shown in [Figure 32](#).

Figure 32 iMC homepage



Log in to the iMC and configure SNMP settings for the iMC to find the device. After the device is found, you can manage and maintain the device through the iMC. For example, you can query device information or configure device parameters.

The SNMP settings on the iMC must be the same as those configured on the device. If not, the device cannot be found or managed by the iMC. See the iMC manuals for more information.

Click **Help** in the upper right corner of each configuration page to get corresponding help information.

# User login control

## User login control methods

The device provides the following login control methods.

Login Through	Login control methods	ACL used
Telnet	Configuring source IP-based login control over Telnet users	Basic ACL
	Configuring source and destination IP-based login control over Telnet users	Advanced ACL
	Configuring source MAC-based login control over Telnet users	Ethernet frame header ACL
NMS	Configuring source IP-based login control over NMS users	Basic ACL
Web	Configuring source IP-based login control over web users	Basic ACL

## Configuring login control over Telnet users

### Configuration preparation

Before configuration, determine the permitted or denied source IP addresses, source MAC addresses, and destination IP addresses.

### Configuring source IP-based login control over Telnet users

Because basic ACLs match the source IP addresses of packets, you can use basic ACLs to implement source IP-based login control over Telnet users. Basic ACLs are numbered from 2000 to 2999. For more information about ACL, see the *ACL and QoS Configuration Guide*.

Follow these steps to configure source IP-based login control over Telnet users:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Create a basic ACL and enter its view, or enter the view of an existing basic ACL	<b>acl [ ipv6 ] number <i>acl-number</i></b> <b>[ match-order { config   auto } ]</b>	Required By default, no basic ACL exists.
Configure rules for this ACL	<b>rule [ <i>rule-id</i> ] { permit   deny }</b> <b>[ source { <i>sour-addr</i> <i>sour-wildcard</i></b> <b>  any }   time-range <i>time-name</i>  </b> <b>fragment   logging ]*</b>	Required
Exit the basic ACL view	<b>quit</b>	—

To do...	Use the command...	Remarks
Enter user interface view	<b>user-interface</b> [ <i>type</i> ] <i>first-number</i> [ <i>last-number</i> ]	—
Use the ACL to control user login by source IP address	<b>acl</b> [ <b>ipv6</b> ] <i>acl-number</i> { <b>inbound</b>   <b>outbound</b> }	Required <b>inbound</b> : Filters incoming Telnet packets. <b>outbound</b> : Filters outgoing Telnet packets.

## Configuring source and destination IP-based login control over Telnet users

Because advanced ACLs can match both source and destination IP addresses of packets, you can use advanced ACLs to implement source and destination IP-based login control over Telnet users. Advanced ACLs are numbered from 3000 to 3999. For more information about ACL, see the *ACL and QoS Configuration Guide*.

Follow these steps to configure source and destination IP-based login control over Telnet users:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Create an advanced ACL and enter its view, or enter the view of an existing advanced ACL	<b>acl</b> [ <b>ipv6</b> ] <b>number</b> <i>acl-number</i> [ <b>match-order</b> { <b>config</b>   <b>auto</b> } ]	Required By default, no advanced ACL exists.
Configure rules for the ACL	<b>rule</b> [ <i>rule-id</i> ] { <b>permit</b>   <b>deny</b> } <i>rule-string</i>	Required
Exit advanced ACL view	<b>quit</b>	—
Enter user interface	<b>user-interface</b> [ <i>type</i> ] <i>first-number</i> [ <i>last-number</i> ]	—
Use the ACL to control user login by source and destination IP addresses	<b>acl</b> [ <b>ipv6</b> ] <i>acl-number</i> { <b>inbound</b>   <b>outbound</b> }	Required <b>inbound</b> : Filters incoming Telnet packets. <b>outbound</b> : Filters outgoing Telnet packets.

## Configuring source MAC-based login control over Telnet users

Ethernet frame header ACLs can match the source MAC addresses of packets, so you can use Ethernet frame header ACLs to implement source MAC-based login control over Telnet users. Ethernet frame header ACLs are numbered from 4000 to 4999. For more information about ACL, see the *ACL and QoS Configuration Guide*.

Follow these steps to configure source MAC-based login control over Telnet users:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—

To do...	Use the command...	Remarks
Create an Ethernet frame header ACL and enter its view	<b>acl number</b> <i>acl-number</i> [ <b>match-order</b> { <b>config</b>   <b>auto</b> } ]	Required By default, no advanced ACL exists.
Configure rules for the ACL	<b>rule</b> [ <i>rule-id</i> ] { <b>permit</b>   <b>deny</b> } <i>rule-string</i>	Required
Exit the advanced ACL view	<b>quit</b>	—
Enter user interface view	<b>user-interface</b> [ <i>type</i> ] <i>first-number</i> [ <i>last-number</i> ]	—
Use the ACL to control user login by source MAC address	<b>acl</b> <i>acl-number</i> <b>inbound</b>	Required <b>inbound</b> : Filters incoming Telnet packets.

#### NOTE:

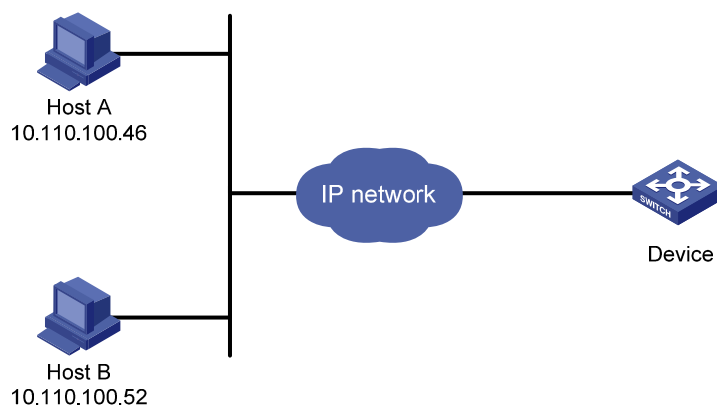
The above configuration does not take effect if the Telnet client and server are not in the same subnet.

## Source MAC-based login control configuration example

### Network requirements

As shown in Figure 33, configure an ACL on the Device to permit only incoming Telnet packets sourced from Host A and Host B.

Figure 33 Network diagram for configuring source MAC-based login control



### Configuration procedure

# Configure basic ACL 2000, and configure rule 1 to permit packets sourced from Host B, and rule 2 to permit packets sourced from Host A.

```

<Sysname> system-view
[Sysname] acl number 2000 match-order config
[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[Sysname-acl-basic-2000] rule 2 permit source 10.110.100.46 0
[Sysname-acl-basic-2000] quit
  
```

# Reference ACL 2000 in user interface view to allow Telnet users from Host A and Host B to access the Device.

```
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] acl 2000 inbound
```

## Configuring source IP-based login control over NMS users

You can log in to the NMS to remotely manage the devices. SNMP is used for communication between the NMS and the agent that resides in the device. By using the ACL, you can control SNMP user access to the device.

### Configuration preparation

Before configuration, determine the permitted or denied source IP addresses.

## Configuring source IP-based login control over NMS users

Because basic ACLs match the source IP addresses of packets, you can use basic ACLs to implement source IP-based login control over NMS users. Basic ACLs are numbered from 2000 to 2999. For more information about ACL, see the *ACL and QoS Configuration Guide*.

Follow these steps to configure source IP-based login control over NMS users:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Create a basic ACL and enter its view, or enter the view of an existing basic ACL	<b>acl [ ipv6 ] number <i>acl-number</i></b> <b>[ match-order { config   auto } ]</b>	Required By default, no basic ACL exists.
Create rules for this ACL	<b>rule [ <i>rule-id</i> ] { permit   deny }</b> <b>[ source { <i>sour-addr</i> <i>sour-wildcard</i>  </b> <b>any }   time-range <i>time-name</i>  </b> <b>fragment   logging ]*</b>	Required
Exit the basic ACL view	<b>quit</b>	—
Associate this SNMP community with the ACL	<b>snmp-agent community { read  </b> <b>write } <i>community-name</i> [ acl</b> <b><i>acl-number</i>   mib-view</b> <b><i>view-name</i> ]*</b>	Required You can associate the ACL when creating the community, the SNMP group, and the user.
Associate the SNMP group with the ACL	<b>snmp-agent group { v1   v2c }</b> <b><i>group-name</i> [ read-view</b> <b><i>read-view</i> ] [ write-view</b> <b><i>write-view</i> ] [ notify-view</b> <b><i>notify-view</i> ] [ acl <i>acl-number</i> ]</b> <b>snmp-agent group v3 <i>group-name</i></b> <b>[ authentication   privacy ]</b> <b>[ read-view <i>read-view</i> ]</b> <b>[ write-view <i>write-view</i> ]</b> <b>[ notify-view <i>notify-view</i> ] [ acl</b> <b><i>acl-number</i> ]</b>	For more information about SNMP, see the <i>Network Management and Monitoring Configuration Guide</i> .



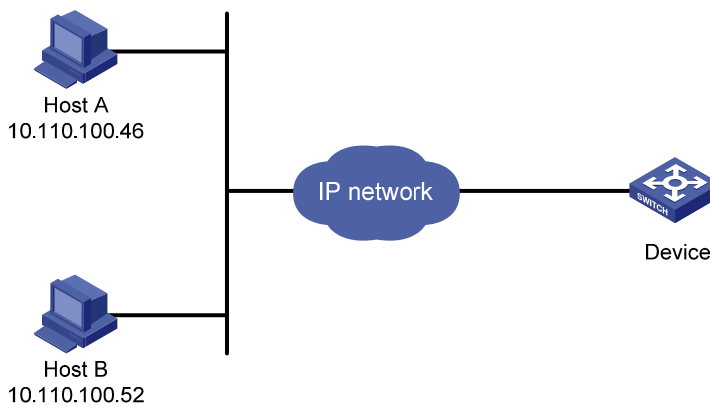
To do...	Use the command...	Remarks
Associate the user with the ACL	<pre>snmp-agent usm-user { v1   v2c } user-name group-name [ acl acl-number ]</pre>	
	<pre>snmp-agent usm-user v3 user-name group-name [ [ cipher ] authentication-mode { md5   sha } auth-password [ privacy-mode { 3des   aes128   des56 } priv-password ] ] [ acl acl-number ]</pre>	

## Source IP-based login control over NMS users configuration example

### Network requirements

As shown in Figure 34, configure the device to allow only NMS users from Host A and Host B to access.

Figure 34 Network diagram for configuring source IP-based login control over NMS users



### Configuration procedure

# Create ACL 2000, and configure rule 1 to permit packets sourced from Host B, and rule 2 to permit packets sourced from Host A.

```
<Sysname> system-view
[Sysname] acl number 2000 match-order config
[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[Sysname-acl-basic-2000] rule 2 permit source 10.110.100.46 0
[Sysname-acl-basic-2000] quit
```

# Associate the ACL with the SNMP community and the SNMP group.

```
[Sysname] snmp-agent community read aaa acl 2000
[Sysname] snmp-agent group v2c groupa acl 2000
[Sysname] snmp-agent usm-user v2c usera groupa acl 2000
```

# Configuring source IP-based login control over web users

You can log in to the web management page of the device through HTTP/HTTPS to remotely manage the devices. By using the ACL, you can control web user access to the device.

## Configuration preparation

Before configuration, determine the permitted or denied source IP addresses.

## Configuring source IP-based login control over web users

Because basic ACLs match the source IP addresses of packets, you can use basic ACLs to implement source IP-based login control over web users. Basic ACLs are numbered from 2000 to 2999. For more information about ACL, see the *ACL and QoS Configuration Guide*.

Follow these steps to configure source IP-based login control over web users:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Create a basic ACL and enter its view, or enter the view of an existing basic ACL	<b>acl [ ipv6 ] number <i>acl-number</i></b> <b>[ match-order { config   auto } ]</b>	Required By default, no basic ACL exists.
Create rules for this ACL	<b>rule [ <i>rule-id</i> ] { permit   deny }</b> <b>[ source { <i>sour-addr</i> <i>sour-wildcard</i></b> <b>  any }   time-range <i>time-name</i>  </b> <b>fragment   logging ]*</b>	Required
Exit the basic ACL view	<b>quit</b>	—
Associate the HTTP service with the ACL	<b>ip http acl <i>acl-number</i></b>	Required to use one command
Associate the HTTPS service with the ACL	<b>ip https acl <i>acl-number</i></b>	

## Logging off online web users

Follow the step to log off online web users:

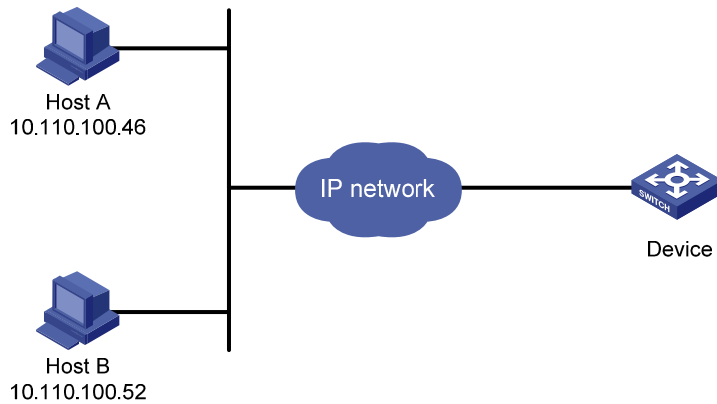
To do...	Use the command...	Remarks
Log off online web users	<b>free web-users { all   user-id</b> <b><i>user-id</i>   user-name <i>user-name</i> }</b>	Required Execute the command in user interface view.

# Source IP-based login control over web users configuration example

## Network requirements

As shown in [Figure 35](#), configure the device to allow only web users from Host B to access.

**Figure 35 Network diagram for configuring source IP-based login control**



## Configuration procedure

# Create ACL 2000, and configure rule 1 to permit packets sourced from Host B.

```
<Sysname> system-view
```

```
[Sysname] acl number 2030 match-order config
```

```
[Sysname-acl-basic-2030] rule 1 permit source 10.110.100.52 0
```

# Associate the ACL with the HTTP service so that only web users from Host B are allowed to access the device.

```
[Sysname] ip http acl 2030
```

# FTP configuration

## FTP overview

### Introduction to FTP

The File Transfer Protocol (FTP) is an application layer protocol for sharing files between server and client over a TCP/IP network.

FTP uses TCP ports 20 and 21 for file transfer. Port 20 is used to transmit data, and port 21 to transmit control commands. For more information about FTP basic operations, see RFC 959.

FTP transfers files in the following modes:

- Binary mode: Transfers files as raw data, such as **.app**, **.bin**, and **.btm** files.
- ASCII mode: Transfers files as text, such as **.txt**, **.bat**, and **.cfg** files.

### FTP operation

FTP adopts the client/server model. Your device can function either as the client or the server. See [Figure 36](#).

- When the device serves as the FTP client, use Telnet or an emulation program to log in to the device from the PC, execute the **ftp** command to establish a connection from the device (FTP client) to the PC (FTP server), and then upload/download files to/from the server.
- When the device serves as the FTP server, run the FTP client program on the PC to establish a connection to the FTP server and upload/download files to/from the server.

**Figure 36 Network diagram for FTP**



When the device serves as the FTP client, you need to perform the following configuration:

**Table 8 Configuration when the device serves as the FTP client**

Device	Configuration	Remarks
Device (FTP client)	Use the <b>ftp</b> command to establish the connection to the remote FTP server	If the remote FTP server supports anonymous FTP, the device can log in to it directly; if not, the device must obtain the FTP username and password first to log in to the remote FTP server.
PC (FTP server)	Enable FTP server on the PC, and configure the username, password, user privilege level, and so on.	—

When the device serves as the FTP server, you need to perform the following configuration:

**Table 9 Configuration when the device serves as the FTP server**

Device	Configuration	Remarks
Device (FTP server)	Enable the FTP server function	Disabled by default. You can use the <b>display ftp-server</b> command to view the FTP server configuration on the device.
	Configure authentication and authorization	Configure the username, password, and authorized directory for an FTP user. The device does not support anonymous FTP for security reasons. You must set a valid username and password. By default, authenticated users can access the root directory of the device.
	Configure the FTP server operating parameters	Parameters such as the FTP connection timeout time
PC (FTP client)	Use the FTP client program to log in to the FTP server.	You can log in to the FTP server only after you input the correct FTP username and password.

**△ CAUTION:**

- Make sure that the FTP server and the FTP client can reach each other before establishing the FTP connection.
- When you use IE to log in to the device serving as the FTP server, some FTP functions are not available. This is because multiple connections are established during the login process but the device supports only one connection at a time.

## Configuring the FTP client

**NOTE:**

Only manage level users can use the **ftp** command to log in to an FTP server, enter FTP client view, and execute directory and file related commands. However, whether the commands can be executed successfully depends on the FTP server authorizations.

## Establishing an FTP connection

Before you can access the FTP server, you must first establish a connection from the FTP client to the FTP server. You can either use the **ftp** command to establish the connection directly or use the **open** command in FTP client view to establish the connection.

When using the **ftp** command, you can specify the source interface (such as a loopback) or source IP address. The primary IP address of the specified source interface or the specified source IP address is used as the source IP address of sent FTP packets. The source address of the transmitted packets is selected following these rules:

- If no source address is specified, the FTP client uses the interface's IP address determined by the matched route as the source IP address to communicate with an FTP server.
- If the source address is specified with the **ftp client source** or **ftp** command, this source address is used to communicate with an FTP server.

- If you use the **ftp client source** command and the **ftp** command to specify a source address respectively, the source address specified with the **ftp** command is used to communicate with an FTP server.
- The source address specified with the **ftp client source** command is valid for all FTP connections and the source address specified with the **ftp** command is valid only for the current FTP connection.

Follow these steps to establish an IPv4 FTP connection:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Configure the source address of the FTP client	<b>ftp client source</b> { <b>interface</b> <i>interface-type</i> <i>interface-number</i>   <b>ip</b> <i>source-ip-address</i> }	Optional A switch uses the IP address of the interface determined by the matched route as the source IP address to communicate with the FTP server by default.
Exit to system view	<b>quit</b>	—
Log in to the remote FTP server directly in user view	<b>ftp</b> [ <i>server-address</i> [ <i>service-port</i> ] [ <b>source</b> { <b>interface</b> <i>interface-type</i> <i>interface-number</i>   <b>ip</b> <i>source-ip-address</i> } ] ]	Use either approach. The <b>ftp</b> command is available in user view, and the <b>open</b> command is available in FTP client view.
Log in to the remote FTP server indirectly in FTP client view	<b>ftp</b> <b>open</b> <i>server-address</i> [ <i>service-port</i> ]	

#### NOTE:

- If there is not a primary IP address configured on the specified source interface, you cannot establish an FTP connection.
- If you use the **ftp client source** command to configure a source interface and then use it to configure a source IP address, the source IP address overwrites the source interface, and vice versa.

Follow these steps to establish an IPv6 FTP connection:

To do...	Use the command...	Remarks
Log in to the remote FTP server directly in user view	<b>ftp ipv6</b> [ <i>server-address</i> [ <i>service-port</i> ] [ <b>source ipv6</b> <i>source-ipv6-address</i> ] [ <b>-i</b> <i>interface-type</i> <i>interface-number</i> ] ]	Use either approach. The <b>ftp ipv6</b> command is available in user view; and the <b>open ipv6</b> command is available in FTP client view.
Log in to the remote FTP server indirectly in FTP client view	<b>ftp ipv6</b> <b>open ipv6</b> <i>server-address</i> [ <i>service-port</i> ] [ <b>-i</b> <i>interface-type</i> <i>interface-number</i> ]	

## Operating the directories on an FTP server

After the switch serving as the FTP client has established a connection with an FTP server, you can create or delete folders under the authorized directory of the FTP server. For more information about establishing an FTP connection, see [“Establishing an FTP connection.”](#)

Follow these steps to operate the directories on an FTP server:

To do...	Use the command...	Remarks
Display detailed information about a directory or file on the remote FTP server	<b>dir</b> [ <i>remotefile</i> [ <i>localfile</i> ] ]	Optional
Query a directory or file on the remote FTP server	<b>ls</b> [ <i>remotefile</i> [ <i>localfile</i> ] ]	Optional
Change the working directory of the remote FTP server	<b>cd</b> { <i>directory</i>   ..   / }	Optional
Exit the current working directory and return to an upper level directory of the remote FTP server	<b>cdup</b>	Optional
Display the working directory that is being accessed	<b>pwd</b>	Optional
Create a directory on the remote FTP server	<b>mkdir</b> <i>directory</i>	Optional
Remove the specified working directory on the remote FTP server	<b>rmdir</b> <i>directory</i>	Optional

## Operating the files on an FTP server

After the switch serving as the FTP client has established a connection with an FTP server, you can upload a file to or download a file from the FTP server under the authorized directory of the FTP server by following these steps. For information about establishing an FTP connection, see [“Establishing an FTP connection.”](#)

1. Use the **dir** or **ls** command to display the directory and the location of the file on the FTP server.
2. Delete useless files for effective use of the storage space.
3. Set the file transfer mode. FTP transmits files in two modes: ASCII and binary. ASCII mode transfers files as text. Binary mode transfers files as raw data.
4. Use the **lcd** command to display the local working directory of the FTP client. You can upload the file under this directory, or save the downloaded file under this directory.
5. Upload or download the file.

Follow these steps to operate the files on an FTP server:

To do...	Use the command...	Remarks
Display detailed information about a directory or file on the remote FTP server	<b>dir</b> [ <i>remotefile</i> [ <i>localfile</i> ] ]	Optional The <b>ls</b> command displays the name of a directory or file only, while the <b>dir</b> command displays detailed information such as the file size and creation time.
Query a directory or file on the remote FTP server	<b>ls</b> [ <i>remotefile</i> [ <i>localfile</i> ] ]	Optional The <b>ls</b> command displays the name of a directory or file only, while the <b>dir</b> command displays detailed information such as the file size and creation time.
Delete the specified file on the remote FTP server permanently	<b>delete</b> <i>remotefile</i>	Optional
Set the file transfer mode to ASCII	<b>ascii</b>	Optional ASCII by default.

To do...	Use the command...	Remarks
Set the file transfer mode to binary	<b>binary</b>	Optional ASCII by default.
Set the data transmission mode to passive	<b>passive</b>	Optional Passive by default.
Display the local working directory of the FTP client	<b>lcd</b>	Optional
Upload a file to the FTP server	<b>put</b> <i>localfile</i> [ <i>remotefile</i> ]	Optional
Download a file from the FTP server	<b>get</b> <i>remotefile</i> [ <i>localfile</i> ]	Optional

## Using another username to log in to an FTP server

After the switch serving as the FTP client has established a connection with the FTP server, you can use another username to log in to the FTP server. For more information about establishing an FTP connection, see [“Establishing an FTP connection.”](#)

This feature allows you to switch to different user levels without affecting the current FTP connection; if you input an incorrect username or password, the current connection will be terminated, and you must log in again to access the FTP server.

Follow the step below to use another username to log in to the FTP server:

To do...	Use the command...	Remarks
Use another username to re-log in after successfully logging in to the FTP server	<b>user</b> <i>username</i> [ <i>password</i> ]	Optional

## Maintaining and debugging an FTP connection

After a switch serving as the FTP client has established a connection with the FTP server, you can perform the following operations to locate and diagnose problems encountered in an FTP connection. For more information about establishing an FTP connection, see [“Establishing an FTP connection.”](#)

To do...	Use the command...	Remarks
Display the help information of FTP-related commands supported by the remote FTP server	<b>remotehelp</b> [ <i>protocol-command</i> ]	Optional
Enable information display in a detailed manner	<b>verbose</b>	Optional Enabled by default
Enable FTP related debugging when the switch acts as the FTP client	<b>debugging</b>	Optional Disabled by default

## Terminating an FTP connection

After the switch serving as the FTP client has established a connection with the FTP server, you can use any of the following commands to terminate an FTP connection. For more information about establishing an FTP connection, see [“Establishing an FTP connection.”](#)



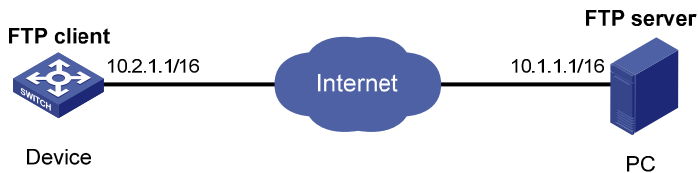
To do...	Use the command...	Remarks
Terminate the connection to the FTP server without exiting FTP client view	<b>disconnect</b>	Optional Equal to the <b>close</b> command.
Terminate the connection to the FTP server without exiting FTP client view	<b>close</b>	Optional Equal to the <b>disconnect</b> command.
Terminate the connection to the FTP server and return to user view	<b>bye</b>	Optional Equal to the <b>quit</b> command in FTP client view.
Terminate the connection to the FTP server and return to user view	<b>quit</b>	Optional Available in FTP client view, equal to the <b>bye</b> command.

## FTP client configuration example

### Network requirements

- As shown in Figure 37, use the device as an FTP client and the PC as the FTP server. Their IP addresses are 10.2.1.1/16 and 10.1.1.1/16 respectively. The device and PC can reach each other.
- The device downloads a system software image file from the PC for device upgrade, and uploads the configuration file to the PC for backup.
- On the PC, an FTP user account has been created for the FTP client, with the username **abc** and the password **pwd**.

Figure 37 Network diagram for FTPing a system software image file from an FTP server



### Configuration procedure

#### ⚠ CAUTION:

If the available memory space of the device is not enough, use the **fixdisk** command to clear the memory or use the **delete /unreserved file-url** command to delete the files not in use and then perform the following operations.

```

# Log in to the server through FTP.
<Sysname> ftp 10.1.1.1
Trying 10.1.1.1
Connected to 10.1.1.1
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(10.1.1.1:(none)):abc
331 Give me your password, please
Password:
  
```

```

230 Logged in successfully

# Set the file transfer mode to binary to transmit system software image file.
[ftp] binary
200 Type set to I.

# Download the system software image file newest.bin from the PC to the device.
[ftp] get newest.bin

# Upload the configuration file config.cfg of the device to the server for backup.
[ftp] ascii
[ftp] put config.cfg back-config.cfg
227 Entering Passive Mode (10,1,1,1,4,2).
125 ASCII mode data connection already open, transfer starting for /config.cfg.
226 Transfer complete.
FTP: 3494 byte(s) sent in 5.646 second(s), 618.00 byte(s)/sec.
[ftp] bye

# Specify newest.bin as the main system software image file for next startup.
<Sysname> boot-loader file newest.bin main

# Reboot the device, and the system software image file is updated at the system reboot.
<Sysname> reboot

```

---

**CAUTION:**

The system software image file for next startup must be saved in the storage medium's root directory. You can copy or move a file to the storage medium's root directory. For more information about the **boot-loader** command, see the *Fundamentals Command Reference*.

---

## Configuring the FTP server

### Configuring FTP server operating parameters

The FTP server uses one of the following modes to update a file when you upload the file (use the **put** command) to the FTP server:

- In fast mode, the FTP server starts writing data to the storage medium after a file is transferred to the memory. This prevents the existing file on the FTP server from being corrupted in the event that anomaly, such as a power failure occurs during a file transfer.
- In normal mode, the FTP server writes data to the storage medium while receiving data. This means that any anomaly, such as a power failure during file transfer might result in file corruption on the FTP server. This mode, however, consumes less memory space than the fast mode.

Follow these steps to configure the FTP server:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enable the FTP server	<b>ftp server enable</b>	Required Disabled by default.

To do...	Use the command...	Remarks
Use an ACL to control FTP clients' access to the switch	<b>ftp server acl</b> <i>acl-number</i>	Optional By default, no ACL is used to control FTP clients' access to the switch.
Configure the idle-timeout timer	<b>ftp timeout</b> <i>minutes</i>	Optional 30 minutes by default. Within the idle-timeout time, if there is no information interaction between the FTP server and client, the connection between them is terminated.
Set the file update mode for the FTP server	<b>ftp update</b> { <b>fast</b>   <b>normal</b> }	Optional Normal update is used by default.
Quit to user view	<b>quit</b>	—
Manually release the FTP connection established with the specified username	<b>free ftp user</b> <i>username</i>	Optional Available in user view

## Configuring authentication and authorization on the FTP server

To allow an FTP user to access certain directories on the FTP server, you must create an account for the user, authorizing access to the directories and associating the username and password with the account.

The following configuration is used when the FTP server authenticates and authorizes a local FTP user. If the FTP server needs to authenticate a remote FTP user, you must configure authentication, authorization and accounting (AAA) policy instead of the local user. For detailed configuration, see the *Security Command Reference*.

In local authentication, the switch checks the input username and password against those configured on the switch. In remote authentication, the switch sends the input username and password to the remote authentication server, which then checks whether they are consistent with those configured on the switch.

Follow these steps to configure authentication and authorization for FTP server:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Create a local user and enter its view	<b>local-user</b> <i>user-name</i>	Required No local user exists by default, and the system does not support FTP anonymous user access.
Assign a password to the user	<b>password</b> { <b>simple</b>   <b>cipher</b> } <i>password</i>	Required
Assign the FTP service to the user	<b>service-type ftp</b>	Required By default, the system does not support anonymous FTP access, and does not assign any service. If the FTP service is assigned, the root directory of the switch is used by default.

To do...	Use the command...	Remarks
Configure user properties	<b>authorization-attribute</b> { <b>acl</b> <i>acl-number</i>   <b>callback-number</b> <i>callback-number</i>   <b>idle-cut</b> <i>minute</i>   <b>level</b> <i>level</i>   <b>user-profile</b> <i>profile-name</i>   <b>user-role</b> <i>security-audit</i>   <b>vlan</b> <i>vlan-id</i>   <b>work-directory</b> <i>directory-name</i> } *	Optional By default, the FTP/SFTP users can access the root directory of the switch, and the user level is 0. You can change the default configuration by using this command.

#### NOTE:

- For more information about the **local-user**, **password**, **service-type ftp**, and **authorization-attribute** commands, see the *Security Command Reference*.
- When the switch serves as the FTP server, if the client is to perform the write operations (such as upload, delete, and create) on the device's file system, the FTP login users must be level 3 users; if the client is to perform other operations such as the read operation, the switch has no restriction on the user level of the FTP login users.

## FTP server configuration example

### Network requirements

- As shown in Figure 38, use the device as an FTP server, and the PC as the FTP client. Their IP addresses are 1.2.1.1/16 and 1.1.1.1/16 respectively. The device and PC can reach each other.
- PC keeps the updated system software image file of the device. Use FTP to upgrade the device and back up the configuration file.
- Set the username to **ftp** and the password to **pwd** for the FTP client to log in to the FTP server.

Figure 38 Upgrading using the FTP server



### Configuration procedure

#### 1. Configure the device (FTP Server)

# Create an FTP user account **ftp**, set its password to **pwd** and the user privilege level to level 3 (the manage level). Allow user **ftp** to access the root directory of the flash, and specify **ftp** to use FTP.

```
<Sysname> system-view
[Sysname] local-user ftp
[Sysname-luser-ftp] password simple pwd
[Sysname-luser-ftp] authorization-attribute level 3
[Sysname-luser-ftp] authorization-attribute work-directory flash:/
[Sysname-luser-ftp] service-type ftp
[Sysname-luser-ftp] quit
```

# Enable FTP server.

```
[Sysname] ftp server enable
[Sysname] quit
```

# Check files on your device. Remove those redundant to ensure adequate space for the system software image file to be uploaded.

```
<Sysname> dir
```

```
Directory of flash:/
```

```
 0  drw-          -  Dec 07 2005 10:00:57  filename
 1  drw-          -  Jan 02 2006 14:27:51  logfile
 2  -rw-         1216  Jan 02 2006 14:28:59  config.cfg
 3  -rw-         1216  Jan 02 2006 16:27:26  back.cfg
```

```
14986 KB total (2511 KB free)
```

```
<Sysname> delete /unreserved flash:/back.cfg
```

## 2. Configure the PC (FTP Client)

# Log in to the FTP server through FTP.

```
c:\> ftp 1.1.1.1
```

```
Connected to 1.1.1.1.
```

```
220 FTP service ready.
```

```
User(1.1.1.1:(none)): ftp
```

```
331 Password required for ftp.
```

```
Password:
```

```
230 User logged in.
```

# Download the configuration file **config.cfg** of the device to the PC for backup.

```
ftp> get config.cfg back-config.cfg
```

# Upload the configuration file **newest.bin** to the device.

```
ftp> put newest.bin
```

```
ftp> bye
```

---

### NOTE:

- You can take the same steps to upgrade configuration file with FTP. When upgrading the configuration file with FTP, put the new file in the storage medium's root directory.
  - After you finish transferring Boot ROM through FTP, you must execute the **bootrom update** command to upgrade Boot ROM.
- 

## 3. Upgrade the device

# Specify **newest.bin** as the main system software image file for next startup.

```
<Sysname> boot-loader file newest.bin main
```

# Reboot the device and the system software image file is updated at the system reboot.

```
<Sysname> reboot
```

---

### ⚠ CAUTION:

The system software image file used for the next startup must be saved in the storage medium's root directory. You can copy or move a file to the storage medium's root directory. For more information about the **boot-loader** command, see the *Fundamentals Command Reference*.

---

## Displaying and maintaining FTP

To do...	Use the command...	Remarks
Display the configuration of the FTP client	<b>display ftp client configuration</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display the configuration of the FTP server	<b>display ftp-server</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display detailed information about logged-in FTP users	<b>display ftp-user</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view

---

# TFTP configuration

## TFTP overview

### Introduction to TFTP

The Trivial File Transfer Protocol (TFTP) provides functions similar to those provided by FTP, but it is less complex than FTP in interactive access interface and authentication. It is more suitable in environments where complex interaction is not needed between client and server.

TFTP uses the UDP port 69 for data transmission. For more information about TFTP basic operation, see RFC 1350.

In TFTP, file transfer is initiated by the client.

- In a normal file downloading process, the client sends a read request to the TFTP server, receives data from the server, and then sends the acknowledgement to the server.
- In a normal file uploading process, the client sends a write request to the TFTP server, sends data to the server, and receives the acknowledgement from the server.

TFTP transfers files in the following modes:

- Binary mode: Transfers files as raw data, such as **.app**, **.bin**, and **.btm** files.
- ASCII mode: Transfers files as text, such as **.txt**, **.bat**, and **.cfg** files.

## TFTP operation

---

### NOTE:

Only the TFTP client service is available with your device at present.

---

**Figure 39 TFTP configuration diagram**



Before using TFTP, the administrator needs to configure IP addresses for the TFTP client and server, and make sure that there is a reachable route between the TFTP client and server.

When the device serves as the TFTP client, you need to perform the following configuration:

**Table 10 Configuration when the device serves as the TFTP client**

Device	Configuration	Remarks
Device (TFTP client)	<ul style="list-style-type: none"> <li>Configure the IP address and routing function, and ensure that the route between the device and the TFTP server is available.</li> <li>Use the <b>ftfp</b> command to establish a connection to the remote TFTP server to upload/download files to/from the TFTP server</li> </ul>	—
PC (TFTP server)	Enable TFTP server on the PC, and configure the TFTP working directory.	—

## Configuring the TFTP client

When a device acts as a TFTP client, you can upload a file on the device to a TFTP server or download a file from the TFTP server to the local device. You can use either of the following methods to download a file:

- Normal download: The device writes the obtained file to the storage medium directly. In this way, if you download a remote file using a filename *destination-filename* that exists in the directory, the device deletes the original file and then saves the new one. If file download fails due to network disconnection or other reasons, the original system file will never recover because it has been deleted.
- Secure download: The device saves the obtained file to its memory and does not write it to the storage medium until the whole file is obtained. If you download a remote file using a filename *destination-filename* that exists in the directory, the original file is not overwritten. If file download fails due to network disconnection or other reasons, the original file still exists. This mode is more secure but consumes more memory.

HP recommends that you use the secure mode or, if you use the normal mode, specify a filename not existing in the current directory as the target filename when downloading the system software image file or the startup configuration file.

Before using the **ftfp** command to establish a TFTP connection, you can perform source address binding. Source address binding means configuring an IP address on a stable interface such as a loopback interface, and then using this IP address as the source IP address of a TFTP connection. The source address binding function simplifies the configuration of ACL rules and security policies. You only need to specify the source or destination address argument in an ACL rule as the address to filter inbound and outbound packets on the device, ignoring the difference between interface IP addresses as well as the effect of interface statuses. You can configure the source address by configuring the source interface or source IP address. The primary IP address configured on the source interface is the source address of the transmitted packets.

Follow these steps to configure the TFTP client:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Use an ACL to control the device's access to TFTP servers	<b>ftfp-server [ ipv6 ] acl <i>acl-number</i></b>	Optional By default, no ACL is used to control the device's access to TFTP servers.



To do...	Use the command...	Remarks
Configure the source address of the TFTP client	<b>tftp client source</b> { <b>interface</b> <i>interface-type interface-number</i>   <b>ip</b> <i>source-ip-address</i> }	Optional A device uses the source address determined by the matched route to communicate with the TFTP server by default.
Return to user view	<b>quit</b>	—
Download or upload a file in an IPv4 network	<b>tftp server-address</b> { <b>get</b>   <b>put</b>   <b>sget</b> } <i>source-filename</i> [ <i>destination-filename</i> ] [ <b>source</b> { <b>interface</b> <i>interface-type interface-number</i>   <b>ip</b> <i>source-ip-address</i> } ]	Optional Available in user view
Download or upload a file in an IPv6 network	<b>tftp ipv6</b> <i>tftp-ipv6-server</i> [ <b>-i</b> <i>interface-type interface-number</i> ] { <b>get</b>   <b>put</b> } <i>source-file</i> [ <i>destination-file</i> ]	Optional Available in user view

#### NOTE:

- If no primary IP address is configured on the source interface, no TFTP connection can be established.
- If you use the **tftp client source** command to first configure the source interface and then the source IP address of the packets of the TFTP client, the new source IP address will overwrite the current one, and vice versa.

## Displaying and maintaining the TFTP client

To do...	Use the command...	Remarks
Display the configuration of the TFTP client	<b>display tftp client configuration</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view

## TFTP client configuration example

### Network requirements

- As shown in Figure 40, use a PC as the TFTP server and the device as the TFTP client. Their IP addresses are 1.2.1.1/16 and 1.1.1.1/16 respectively. The device and PC can reach each other.
- The device downloads a system software image file from PC for upgrading and uploads a configuration file named **config.cfg** to PC for backup.

Figure 40 Smooth upgrading using the TFTP client function



## Configuration procedure

1. Configure the PC (TFTP Server), the configuration procedure is omitted.
  - On the PC, enable the TFTP server
  - Configure a TFTP working directory
2. Configure the device (TFTP Client)

---

### △ CAUTION:

If the available memory space of the device is not enough, use the **fixdisk** command to clear the memory or use the **delete /unreserved file-ur/** command to delete the files not in use and then perform the following operations.

---

# Enter system view.

```
<Sysname> system-view
```

# Download system software image file **newest.bin** from the PC.

```
<Sysname> tftp 1.2.1.1 get newest.bin
```

# Upload a configuration file **config.cfg** to the TFTP server.

```
<Sysname> tftp 1.2.1.1 put config.cfg configback.cfg
```

# Specify **newest.bin** as the main system software image file for the next startup.

```
<Sysname> boot-loader file newest.bin bbb.bin main
```

# Reboot the device and the system software image file is upgraded.

```
<Sysname> reboot
```

---

### △ CAUTION:

The system software image file used for the next startup must be saved in the storage medium's root directory of the. You can copy or move a file to the root directory of the storage medium. For more information about the **boot-loader** command, see the *Fundamentals Command Reference*.

---

---

# File management

## Managing files

Files such as host software and configuration files that are necessary for the operation of the device are saved in the storage media of the device. You can manage files on your device through these operations: [Performing directory operations](#), [Performing file operations](#), [Performing batch operations](#), [Performing storage medium operations](#), [Setting prompt modes](#), [Setting prompt modes](#), [Setting prompt modes](#), [Setting prompt modes](#), and [Setting prompt modes](#).

## Filename formats

When you specify a file, you must enter the filename in one of the following formats.

Filename formats:

Format	Description	Length	Example
<i>file-name</i>	Specifies a file in the current working directory.	1 to 91 characters	a.cfg indicates a file named <b>a.cfg</b> in the current working directory
<i>path/file-name</i>	Specifies a file in the specified folder in the current working directory. <i>path</i> indicates the name of the folder. You can specify multiple folders, indicating a file under a multi-level folder.	1 to 135 characters	test/a.cfg indicates a file named <b>a.cfg</b> in the <b>test</b> folder in the current working directory.
<i>drive:[path]/file-name</i>	Specifies a file in the specified storage medium on the device. <i>drive</i> represents the storage medium name, which is usually <b>flash</b> or <b>cf</b> . If there is only one storage medium on the device, you do not need to provide information about the storage medium. If multiple storage media exist on the device, you must provide the related information to identify the storage medium.	1 to 135 characters	flash:/test/a.cfg indicates a file named <b>a.cfg</b> in the <b>test</b> folder in the root directory of the flash memory.

## Performing directory operations

You can create or remove a directory, display the current working directory, the specified directory, and file information.

## Displaying directory information

To do...	Use the command...	Remarks
Display directory or file information	<code>dir [ /all ] [ file-url ]</code>	Required Available in user view

## Displaying the current working directory

To do...	Use the command...	Remarks
Display the current working directory	<code>pwd</code>	Required Available in user view

## Changing the current working directory

To do...	Use the command...	Remarks
Change the current working directory	<code>cd { directory   ..   / }</code>	Required Available in user view

## Creating a directory

To do...	Use the command...	Remarks
Create a directory	<code>mkdir directory</code>	Required Available in user view

## Removing a directory

To do...	Use the command...	Remarks
Remove a directory	<code>rmdir directory</code>	Required Available in user view

### NOTE:

- The directory to be removed must be empty, meaning that before you remove a directory, you must delete all the files and the subdirectory in this directory. For file deletion, see the **delete** command; for subdirectory deletion, see the **rmdir** command.
- The **rmdir** command automatically deletes the files in the recycle bin in the current directory.

## Performing file operations

You can display the specified directory or file information; display file contents; rename, copy, move, remove, restore, and delete files.

---

**NOTE:**

You can create a file by copying, downloading or using the **save** command.

---

## Displaying file information

To do...	Use the command...	Remarks
Display file or directory information	<b>dir</b> [ /all ] [ <i>file-url</i> ]	Required Available in user view

## Displaying the contents of a file

To do...	Use the command...	Remarks
Display the contents of a file	<b>more</b> <i>file-url</i>	Required Only text files can be displayed. Available in user view

## Renaming a file

To do...	Use the command...	Remarks
Rename a file	<b>rename</b> <i>fileurl-source fileurl-dest</i>	Required Available in user view

## Copying a file

To do...	Use the command...	Remarks
Copy a file	<b>copy</b> <i>fileurl-source fileurl-dest</i>	Required Available in user view

## Moving a file

To do...	Use the command...	Remarks
Move a file	<b>move</b> <i>fileurl-source fileurl-dest</i>	Required Available in user view

## Deleting a file

To do...	Use the command...	Remarks
Move a file to the recycle bin or delete it permanently	<b>delete</b> [ /unreserved ] <i>file-url</i>	Required Available in user view

**CAUTION:**

- The files in the recycle bin still occupy storage space. To delete a file in the recycle bin, execute the **reset recycle-bin** command in the directory to which the file originally belongs. HP recommends you to empty the recycle bin periodically with the **reset recycle-bin** command to save storage space.
- The **delete /unreserved file-url** command deletes a file permanently and the action cannot be undone. Executing this command equals executing the **delete file-url** command and then the **reset recycle-bin** command in the same directory.

## Restoring a file from the recycle bin

To do...	Use the command...	Remarks
Restore a file from the recycle bin	<b>undelete</b> <i>file-url</i>	Required Available in user view

## Emptying the recycle bin

To do...	Use the command...	Remarks
Enter the original working directory of the file to be deleted	<b>cd</b> { <i>directory</i>   ..   / }	Optional If the original directory of the file to be deleted is not the current working directory, this command is required. Available in user view
Delete the file in the current directory and in the recycle bin	<b>reset recycle-bin</b> [ /force ]	Required Available in user view

## Performing batch operations

A batch file is a set of executable commands. Executing a batch file is the same as executing the commands in the batch file one by one.

Before executing a batch file, edit the batch file on your PC, and then download the batch file to the device. If the suffix of the file is not **.bat**, use the **rename** command to change the suffix to **.bat**.

Follow these steps to execute a batch file:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Execute a batch file	<b>execute</b> <i>filename</i>	Required

**CAUTION:**

Executing a batch file does not guarantee successful execution of every command in the batch file. If a command has error settings or the conditions for executing the command are not satisfied, this command fails to be executed, and the system skips to the next command.

# Performing storage medium operations

## Managing the space of a storage medium

When the space of a storage medium becomes inaccessible due to abnormal operations, you can use the **fixdisk** command to restore it. The execution of the **format** command formats the storage medium, and all the data on the storage medium is deleted.

Use the following commands to manage the space of a storage medium:

To do...	Use the command...	Remarks
Restore the space of a storage medium	<b>fixdisk</b> <i>device</i>	Optional Available in user view
Format a storage medium	<b>format</b> <i>device</i>	Optional Available in user view

### CAUTION:

When you format a storage medium, all the files stored on it are erased and cannot be restored. If a startup configuration file exists on the storage medium, formatting the storage medium results in loss of the startup configuration file.

## Setting prompt modes

The system provides the following prompt modes:

- **alert**—In this mode, the system warns you about operations that may bring undesirable consequences such as file corruption or data loss.
- **quiet**—In this mode, the system does not prompt confirmation for any operation.

To prevent undesirable consequences resulting from mis-operations, the **alert** mode is preferred.

Follow these steps to set the operation prompt mode:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Set the operation prompt mode of the file system	<b>file prompt { alert   quiet }</b>	Optional The default is <b>alert</b> .

## Example for file operations

```
# Display the files and the subdirectories in the current directory.
```

```
<Sysname> dir
```

```
Directory of flash:/
```

```
0 drw-          - Feb 16 2006 11:45:36 logfile
```

```
1  -rw-      1218  Feb 16 2006 11:46:19  config.cfg
2  drw-          -  Feb 16 2006 15:20:27  test
3  -rw-     184108  Feb 16 2006 15:30:20  aaa.bin
```

14986 KB total (2521 KB free)

# Create a new folder **mytest** in the test directory.

```
<Sysname> cd test
```

```
<Sysname> mkdir mytest
```

```
%Created dir flash:/test/mytest.
```

# Display the current working directory.

```
<Sysname> pwd
```

```
flash:/test
```

# Display the files and the subdirectories in the test directory.

```
<Sysname> dir
```

```
Directory of flash:/test/
```

```
0  drw-          -  Feb 16 2006 15:28:14  mytest
```

14986 KB total (2519 KB free)

# Return to the upper directory.

```
<Sysname> cd ..
```

# Display the current working directory.

```
<Sysname> pwd
```

```
flash:
```



---

# Configuration file management

## Configuration file overview

A configuration file contains a set of commands. You can save the current configuration to a configuration file so that the configuration can take effect after a switch reboot. In addition, you can conveniently view the configuration information, or upload and download the configuration file to/from another switch to configure switches in batches.

## Types of configuration

The switch maintains the following types of configurations: factory defaults, startup configuration, and running configuration.

### Factory defaults

Switches are shipped with some basic settings, which are called factory defaults. These default settings ensure that a switch can start up and run normally when it has no configuration file or the configuration file is damaged.

### Startup configuration

Use startup configuration for initialization when the switch boots. If this file does not exist, the system boots using null configuration. Null configuration is the factory default configuration, which may differ from the default settings for commands. The factory default configuration may vary with switch models.

View the startup configuration using either of the following methods:

- Use the **display startup** command to view the currently using configuration file, and use the **more** command to view the content of the configuration file.
- After the reboot of the switch and before configuring the switch, use the **display current-configuration** command to view the startup configuration.

### Running configuration

The running configuration is stored in the temporary storage media of the switch, and will be removed if not saved when the switch reboots.

Use the **display current-configuration** command to view the current validated configuration of the switch.

## Format and content of a configuration file

A configuration file is saved as a text file; the following rules apply:

- Only non-default configuration settings are saved.
- Commands in a configuration file are listed in sections by views, usually in the order of system view, interface view, routing protocol view, and user interface view. Sections are separated with one or multiple blank lines or comment lines that start with a pound sign **#**.
- A configuration file ends with a return.

## Coexistence of multiple configuration files

The switch can save multiple configuration files on its storage media. You can save the configurations used in different networking environments as different configuration files. When the switch moves between networking environments, specify the configuration file as the startup configuration file of the switch and then restart the switch. Multiple configuration files allow the switch to adapt to a network rapidly, saving the configuration workload.

A switch starts up using only one configuration file. However, you can specify two startup configuration files, main startup configuration file and backup startup configuration file as needed when the switch has main and backup configuration files. The switch starts up using the main startup configuration file. If the main startup configuration file is corrupted or lost, the switch starts up using the backup startup configuration file. Switches supporting main and backup startup configuration files are more secure and reliable.

At a moment, the switch has at most one main startup configuration file and one backup startup configuration file. You can specify neither of the two files (displayed as NULL).

You can specify main and backup startup configuration files using one of the following methods:

- Specify them when saving the running configuration. For more information, see [“Saving the running configuration.”](#)
- Specify them when specifying the startup configuration file. For more information, see [“Specifying a startup configuration file to be used at the next system startup.”](#)

## Startup with the configuration file

The switch takes the following steps when it starts up:

1. If the main startup configuration file you specified exists, the switch starts up with this configuration file.
2. If the main startup configuration file you specified does not exist but the backup startup configuration file exists, the switch starts up with the backup startup configuration file.
3. If neither the main nor the backup startup configuration file exists, the switch starts up with null configuration.

## Saving the running configuration

### Introduction

To make configuration changes take effect at the next startup of the switch, save the running configuration to the startup configuration file to be used at the next startup before the switch reboots.

### Modes in saving the configuration

- Fast saving mode. This is the mode when you use the **save** command without the **safely** keyword. The mode saves the file more quickly but is likely to lose the existing configuration file if the switch reboots or the power fails during the process.
- Safe mode. This is the mode when you use the **save** command with the **safely** keyword. The mode saves the file more slowly but can retain the configuration file in the switch even if the switch reboots or the power fails during the process.

The fast saving mode is suitable for environments where the power supply is stable. The safe mode is preferred in environments where a stable power supply is unavailable or remote maintenance is involved.

Follow these steps to save the current configuration:

To do...	Use the command...	Remarks
Save the current configuration to the specified file, but the configuration file will not be set as the file for the next startup	<b>save</b> <i>file-url</i>	Required
Save the current configuration to the root directory of the storage medium and specify the file as the startup configuration file to be used at the next system startup	<b>save</b> [ <b>safely</b> ] [ <b>backup</b>   <b>main</b> ] [ <b>force</b> ]	Use either command Available in any view.

#### NOTE:

- The configuration file must have the **.cfg** extension.
- The execution of the **save** [ **safely** ] and **save** [ **safely** ] **main** commands has the same effect: The system will save the current configuration and specify the configuration file as the main startup configuration file to be used at the next system startup.
- During the execution of the **save** [ **backup** | **main** ] command, the startup configuration file to be used at the next system startup may be lost if the switch reboots or the power supply fails. The switch will boot with the null configuration, and after the switch reboots, you will need to re-specify a startup configuration file for the next system startup (see [“Specifying a startup configuration file to be used at the next system startup”](#)).

## Setting configuration rollback

### Configuration rollback

Configuration rollback allows you to revert to a previous configuration state based on a specified configuration file. The specified configuration file must be a valid **.cfg** file generated by using either the backup function (manually or automatically) or the **save** command, or, if a configuration file is generated by another switch, the configuration file must comply with the format of the configuration file on the current switch. HP recommends that you use the configuration file that is generated by using the backup function (manually or automatically). Configuration rollback can be applied in the following situations:

- Running configuration error. Rolling back the running configuration to a correct one is needed.
- The application environment has changed and the switch has to run in a configuration state based on a previous configuration file without being rebooted.

Before setting configuration rollback, perform the following steps:

1. Specify the filename prefix and path for saving the running configuration.
2. Save the running configuration with the specified filename (filename prefix + serial number) to the specified path. The running configuration can be saved automatically or manually.

When you enter the **configuration replace file** command, the system compares the running configuration and the specified replacement configuration file. The **configuration replace file** command performs the following actions:

- Preserves all commands present in both the replacement configuration file and the running configuration.
- Removes commands from the running configuration that are not present in the replacement configuration file.
- Applies the commands from the replacement configuration file that are not present in the running configuration.
- Applies the commands from the replacement configuration file that have different configurations in the running configuration.

## Configuration task list

Complete these tasks to configure the configuration rollback:

Task	Remarks
Configuring parameters for saving the running configuration	Required
Enabling automatic saving of the running configuration	Required
Manually saving the running configuration	Use either approach
Setting configuration rollback	Required

## Configuring parameters for saving the running configuration

Before the running configuration is saved manually or automatically, the file path and filename prefix must be configured. After that, the system saves the running configuration with the specified filename (filename prefix\_serial number.cfg) to the specified path. The filename of a saved configuration file is like **20080620archive\_1.cfg**, or **20080620archive\_2.cfg**. The saved configuration files are numbered automatically, from 1 to 1,000 (with an increment of 1). If the serial number reaches 1,000, it restarts from 1. If you change the path or filename prefix, or reboot the switch, the saved file serial number restarts from 1, and the system recounts the saved configuration files. If you change the path of the saved configuration files, the files in the original path become common configuration files, and are not processed as saved configuration files, and are not displayed when you view saved configuration files.

The number of saved configuration files has an upper limit. After the maximum number of files is saved, the system deletes the oldest files when the next configuration file is saved.

Follow these steps to configure parameters for saving the running configuration:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Configure the path and filename prefix for saving configuration files	<b>archive configuration location</b> <i>directory filename-prefix</i> <i>filename-prefix</i>	Required By default, the path and filename for saving configuration files are not configured, and the system does not save the configuration file at a specified interval.

To do...	Use the command...	Remarks
Set the maximum number of configuration files that can be saved	<b>archive configuration max</b> <i>file-number</i>	Optional The default number is 5.

**NOTE:**

- If the **undo archive configuration location** command is executed, the running configuration cannot be saved either manually or automatically, and the configuration is restored to the default by executing the **archive configuration interval** and **archive configuration max** commands. The saved configuration files are cleared.
- The value of the *file-number* argument is determined by memory space. Set a comparatively small value for the *file-number* argument if the available memory space is small.

## Enabling automatic saving of the running configuration

You can configure the system to save the running configuration at a specified interval, and use the **display archive configuration** command to view the filenames and save time of the saved configuration files. This enables you to easily roll back the current configuration to a previous configuration state.

Configure an automatic save interval based on the storage media's performance and the frequency of configuration modification using the following guidelines:

- If the configuration of the switch does not change frequently, manually save the running configuration as needed
- Save the running configuration manually, or configure automatic saving with an interval longer than 1,440 minutes (24 hours).

Follow these steps to enable automatic saving of the running configuration:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enable the automatic saving of the running configuration, and set the interval	<b>archive configuration interval</b> <i>minutes</i>	Optional Disabled by default

**NOTE:**

The path and filename prefix for saving configuration files must be specified before you configure the automatic saving period.

## Manually saving the running configuration

Automatic saving of the running configuration occupies system resources, and frequent saving can greatly affect system performance. If the system configuration does not change frequently, disable automatic saving of the running configuration and save it manually.

In addition, automatic saving of the running configuration is performed periodically, while manual saving can be used to immediately save the running configuration. Before performing a complicated configuration, manually save the running configuration so that the switch can revert to the previous state if the configuration fails.

Follow the step below to manually save the running configuration:

To do...	Use the command...	Remarks
Manually save the running configuration	<b>archive configuration</b>	Required Available in user view

**NOTE:**

Specify the path and filename prefix of a save configuration file before you manually save the running configuration; otherwise, the operation fails.

## Setting configuration rollback

Follow these steps to set configuration rollback:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Set configuration rollback	<b>configuration replace file <i>filename</i></b>	Required

 **CAUTION:**

Configuration rollback may fail if one of the following situations is present (if a command cannot be rolled back, the system skips it and processes the next one):

- The complete undo form of a command is not supported. You cannot get the actual undo form of the command by simply putting the keyword **undo** in front of the command, so the complete undo form of the command cannot be recognized by the switch.
- The configuration cannot be removed, such as hardware-related commands
- Commands in different views are dependent on each other
- If the replacement configuration file is not a complete file generated by using the **save** or **archive configuration** command, or the file is copied from a different type of switch, the configuration cannot be rolled back. Ensure that the replacement configuration file is correct and compatible with the current switch.
- The configuration file specified with the **configuration replace file *filename*** command can only be a configuration file in simple text. Otherwise, errors may occur in configuration rollback.

## Specifying a startup configuration file to be used at the next system startup

To specify a startup configuration file to be used at the next system startup, use the following guidelines:

- Use the **save** command. If you save the running configuration to the specified configuration file in the interactive mode, the system automatically sets the file as the main startup configuration file to be used at the next system startup.
- Use the command dedicated to specify a startup configuration file to be used at the next startup, which is described in the following table:

Follow the step below to specify a startup configuration file to be used at the next startup:

To do...	Use the command...	Remarks
Specify a startup configuration file to be used at the next startup	<b>startup saved-configuration</b> <i>cfgfile</i> [ <b>backup</b>   <b>main</b> ]	Required Available in user view

**CAUTION:**

A configuration file must use **.cfg** as its extension name and the startup configuration file must be saved in the storage media's root directory.

## Backing up the startup configuration file

The backup function allows you to copy the startup configuration file to be used at the next startup from the switch to the TFTP server.

The backup operation backs up the main startup configuration file to the TFTP server for switches supporting main and backup startup configuration files.

Follow the step below to back up the startup configuration file to be used at the next startup:

To do...	Use the command...	Remarks
Back up the startup configuration file to be used at the next startup to the specified TFTP server	<b>backup startup-configuration to</b> <i>dest-addr</i> [ <i>dest- filename</i> ]	Required Available in user view

**NOTE:**

Before the backup operation:

- Make sure that the server is reachable and enabled with TFTP service, and the client has the read and write permission.
- Use the **display startup** command (in user view) to check whether you have specified a startup configuration file to be used at the next startup. If the file is set as NULL or does not exist, the backup operation fails.

## Deleting a startup configuration file

You can delete a startup configuration file at the CLI. On a switch that has main and backup startup configuration files, you can choose to delete the main, the backup, or both. If the switch has only one startup configuration to be used at the next startup, the system only sets the startup configuration file to NULL.

You may need to delete a startup configuration file to be used at the next startup for one of the following reasons:

- After you upgrade system software, the existing startup configuration files do not match the new system software.
- Startup configuration files are corrupted (often caused by loading a wrong configuration file).

With startup configuration files deleted, the switch uses null configuration at the next startup.

Follow the step below to delete a startup configuration file to be used at the next startup:

To do...	Use the command...	Remarks
Delete a startup configuration file to be used at the next startup from the storage media	<b>reset saved-configuration</b> [ <b>backup</b>   <b>main</b> ]	Required Available in user view

**CAUTION:**

This command permanently deletes startup configuration files to be used at the next startup from the switch. Use the command with caution.

## Restoring a startup configuration file

The restore function allows you to copy a configuration file from a TFTP server to the switch and specify the file as the startup configuration file to be used at the next startup.

Follow the step below to restore a startup configuration file to be used at the next startup:

To do...	Use the command...	Remarks
Restore a startup configuration file to be used at the next startup	<b>restore startup-configuration from</b> <i>src-addr src-filename</i>	Required Available in user view

**NOTE:**

- The restore operation restores the main startup configuration file.
- Before restoring a configuration file, ensure that the server is reachable, the server is enabled with TFTP service, and the client has read and write permission.
- After execution of the command, use the **display startup** command (in user view) to verify that the filename of the configuration file to be used at the next system startup is the same with that specified by the *filename* argument.

## Displaying and maintaining a configuration file

To do...	Use the command...	Remarks
Display the information about configuration rollback	<b>display archive configuration</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display the factory defaults of the switch	<b>display default-configuration</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display the current validated configurations of the switch	<b>display current-configuration</b> [ [ <b>configuration</b> [ <i>configuration</i> ]   <b>interface</b> [ <i>interface-type</i> ] [ <i>interface-number</i> ]   <b>exclude modules</b> ] [ <b>by-linenum</b> ] [ [ { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ] ]	Available in any view
Display the running configuration file saved on the storage media of the switch	<b>display saved-configuration</b> [ <b>by-linenum</b> ] [ [ { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view



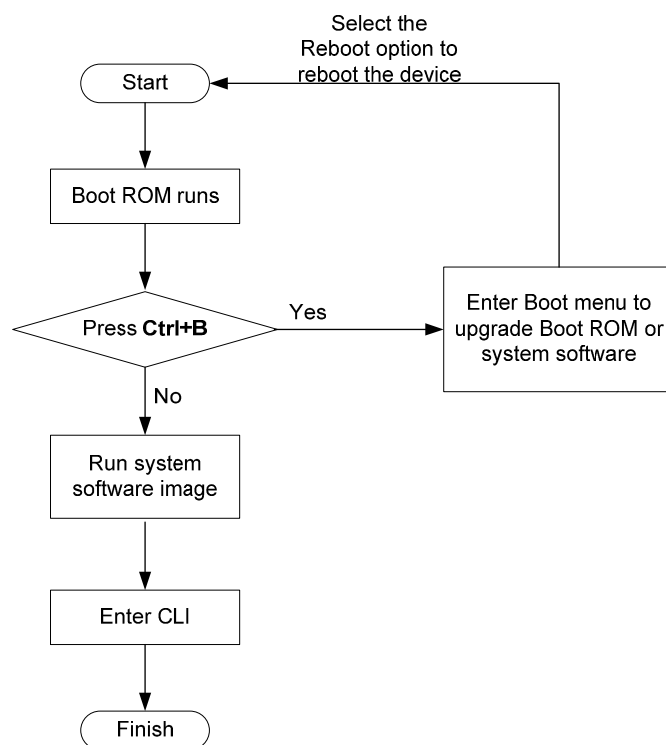
To do...	Use the command...	Remarks
Display the configuration files used at this and the next system startup	<b>display startup</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display the valid configuration under the current view	<b>display this</b> [ <b>by-linenum</b> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view

# Software upgrade configuration

## Switch software overview

Switch software includes the Boot ROM and the system software images. After powered on, the device runs the Boot ROM image, initializes the hardware, and displays the hardware information. Then the device runs the system software image, which provides drivers and adaptation for hardware, and implements service features. The Boot ROM and system software images are required for the startup and running of a device.

**Figure 41 Relationship between the Boot ROM program and the system software images**



## Software upgrade methods

You can upgrade both Boot ROM and system software at the Boot menu or at the command line interface (CLI). The following sections cover how to upgrade them at the CLI. For instructions about how to upgrade them at the Boot menu, see the installation manual of your switch.

Upgrading at the CLI falls into the following categories:

Upgrade method	Upgrade object	Description
<a href="#">Upgrading the Boot ROM program through a system reboot</a>	Boot ROM image	<ul style="list-style-type: none"><li>You need to reboot the whole system to upgrade the software of a switch.</li><li>This causes running service interruption during the</li></ul>

Upgrade method	Upgrade object	Description
Upgrading system software through a system reboot	System software	upgrade process, and is not recommended.
Software upgrade by installing hotfixes	System software	<ul style="list-style-type: none"> <li>Hotfix is a fast, cost-effective method to repair software defects of a switch.</li> <li>Compared with software version upgrade, hotfix can upgrade the software without interrupting the running services of the switch. It can repair the software defects of the current version without rebooting the switch.</li> <li>The patch files match the switch model and software version. If they are not matched, the hotfixing operation fails.</li> </ul>

## Upgrading the Boot ROM program through a system reboot

Follow these steps to upgrade Boot ROM:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enable the validity check function when upgrading Boot ROM	<b>bootrom-update security-check enable</b>	Optional By default, the validity check function is enabled at the time of upgrading Boot ROM.
Return to user view	<b>quit</b>	—
Save the Boot ROM image to the root directory of the Flash of the switch by using FTP, TFTP, or other approaches.	—	Required For more information about FTP or TFTP, see the chapters “FTP configuration” and “TFTP configuration.”
Upgrade Boot ROM on the switch	<b>bootrom update file file-url slot slot-number-list</b>	Required Available in user view.
Reboot the switch	<b>reboot [ slot slot-number ]</b>	The <b>slot</b> keyword specifies the ID of a switch. The ID can only be 1. Available in user view.

### CAUTION:

To execute the **bootrom** command successfully, save the Boot ROM image in the storage media’s root directory on the switch.

# Upgrading system software through a system reboot

Follow these steps to upgrade system software through a system reboot:

To do...	Use the command...	Remarks
Save the system software image to the root directory of the Flash of the switch by using FTP, TFTP, or other approaches.	—	Required For more information about FTP or TFTP, see the chapters “FTP configuration” and “TFTP configuration.”
Specify system software image to be used at the next boot of the switch	<b>boot-loader file</b> <i>file-url slot slot-number</i> { <b>main</b>   <b>backup</b> }	Required Available in user view.
Reboot the switch	<b>reboot</b> [ <b>slot</b> <i>slot-number</i> ]	The <b>slot</b> keyword specifies the ID of a switch. The switch ID can only be 1. Available in user view.

## ⚠ CAUTION:

- You must save the file to be used at the next switch boot in the root directory of the switch. You can copy or move a file to change the path of it to the root directory.
- To execute the **boot-loader** command successfully, save the file to be used at the next device boot in the storage media’s root directory on the switch.

## Software upgrade by installing hotfixes

Hotfix can repair software defects of the current version without rebooting the device, protecting the running services of the device from being interrupted.

### Basic concepts in hotfix

#### Patch and patch file

A patch, also called “*patch unit*”, is a package used to fix software defects. Patches are usually released as patch files. A patch file may contain one or more patches for different defects. After loaded from the storage medium to the memory patch area, each patch is assigned a unique number, which starts from 1, for identification, management and operation. For example, if a patch file has three patch units, they are numbered as 1, 2, and 3 respectively.

#### Incremental patch

An incremental patch means that the patch is dependent on the previous patch units. For example, if a patch file has three patch units, patch 3 can be run only after patch 1 and 2 take effect. You cannot run patch 3 separately.

Currently released patches are all incremental patches.

## Common patch and temporary patch

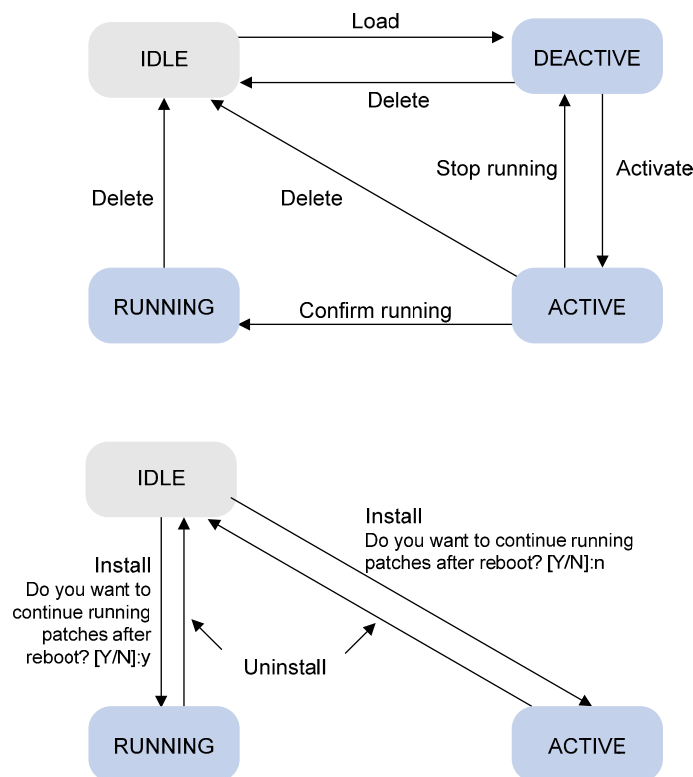
- Common patches are those formally released through the version release flow.
- Temporary patches are those not formally released through the version release flow, but temporarily provided to solve the emergent problems.

Common patches always include the functions of the previous temporary patches so as to replace them. The patch type only affects the patch loading process. The system deletes all of the temporary patches before it loads the common patch.

## Patch status

Each patch has its status, which can be switched only by commands. The relationship between patch state changes and command actions is shown in Figure 42. The patch can be in the state of IDLE, DEACTIVE, ACTIVE, and RUNNING. Load, run temporarily, confirm running, stop running, delete, install, and uninstall represent operations, corresponding to commands of **patch load**, **patch active**, **patch run**, **patch deactivate**, **patch delete**, **patch install**, and **undo patch install**. For example, if you execute the **patch active** command for the patches in the DEACTIVE state, the patches turn to the ACTIVE state.

Figure 42 Relationship between patch state changes and command actions



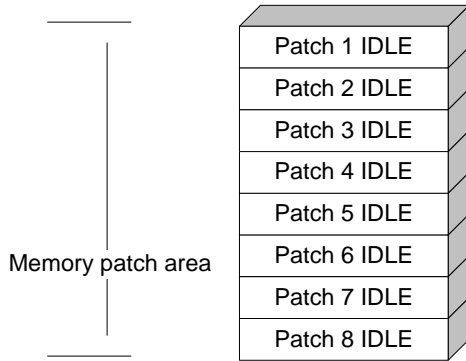
### NOTE:

Information about patch states is saved in the file **patchstate** on the flash. Do not to operate this file.

## IDLE state

Patches in the IDLE state are not loaded. You cannot install or run the patches, as shown in Figure 43 (in this example, the memory patch area can load up to eight patches).

**Figure 43 Patches are not loaded to the memory patch area**



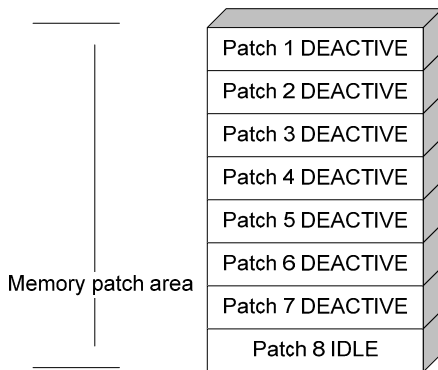
**NOTE:**

The memory patch area supports up to 200 patches.

**DEACTIVE state**

Patches in the DEACTIVE state have been loaded to the memory patch area but have not run in the system yet. Suppose that the patch file to be loaded has seven patches. After the seven patches successfully pass the version check and CRC check, they are loaded to the memory patch area and are in the DEACTIVE state. At this time, the patch states in the system are as shown in [Figure 44](#).

**Figure 44 A patch file is loaded to the memory patch area**

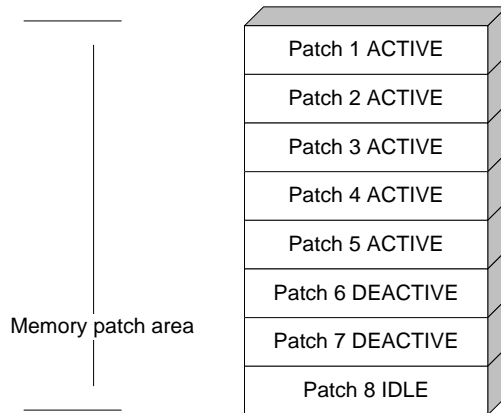


**ACTIVE state**

Patches in the ACTIVE state are those that have run temporarily in the system and become DEACTIVE after system reboot. For the seven patches in [Figure 44](#), if you activate the first five patches, their states change from DEACTIVE to ACTIVE. At this time, the patch states in the system are as shown in [Figure 45](#).

The patches that are in the ACTIVE state are in the DEACTIVE state after system reboot.

**Figure 45 Patches are activated**

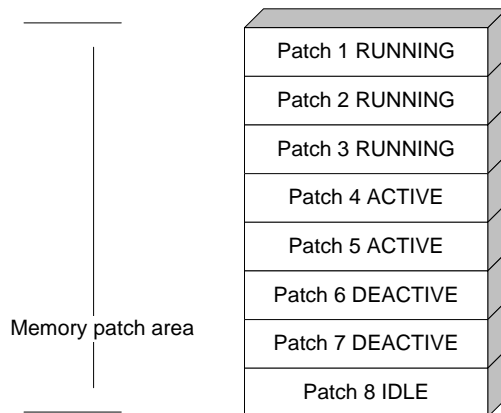


## RUNNING state

After you confirm the ACTIVE patches are running, the patch state becomes RUNNING and they are placed in the RUNNING state after system reboot. For the five patches in [Figure 45](#), if you confirm the first three patches are running, their states change from ACTIVE to RUNNING. At this time, the patch states of the system are as shown in [Figure 46](#).

The patches that are in the RUNNING state are still in the RUNNING state after system reboot.

**Figure 46 Patches are running**



## Configuration prerequisites

Patches are released per switch model. Before patching the system, you need to save the appropriate patch files to the switch's storage media using FTP or TFTP. When saving the patch files, note that the following rules apply:

- The patch files match the switch model and software version. If they are not matched, the hotfix operation fails.
- Name a patch file properly. Otherwise, the system cannot locate the patch file and the hotfixing operation fails. The name is in the format of "patch\_PATCH-FLAG suffix.bin". The PATCH-FLAG is pre-defined and support for the PATCH-FLAG depends on switch model. The first three characters of the version item (using the **display patch information** command) represent the PATCH-FLAG suffix. The system searches the root directory of the storage medium (Flash by default) for patch files based

on the PATCH-FLAG. If there is a match, the system loads patches to or installs them on the memory patch area.

The following table describes the default patch name for the switch series.

PATCH-FLAG	Default patch name
PATCH-311	patch_311.bin

## One-step patch installation

To install patches in one step, use the **patch install** command. After you execute the command, the system displays the message "Do you want to continue running patches after reboot? [Y/N]:"

- Entering **y** or **Y**: All of the specified patches are installed, and turn to the RUNNING state from IDLE. This equals execution of the commands **patch location**, **patch load**, **patch active**, and **patch run**. The patches remain RUNNING after system reboot.
- Entering **n** or **N**: All of the specified patches are installed and turn to the ACTIVE state from IDLE. This equals execution of the commands **patch location**, **patch load** and **patch active**. The patches turn to the DEACTIVE state after system reboot.

Follow these steps to install the patches in one step:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Install the patches in one step	<b>patch install</b> <i>patch-location</i>	Required

### NOTE:

- The patch matches the switch type and software version.
- To uninstall all patches in one operation, use the **undo patch install** command, which has the same effect as [Step-by-step patch uninstallation](#).

## Step-by-step patch installation

Follow these steps to load a patch file:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Configure the patch file location	<b>patch location</b> <i>patch-location</i>	Optional <b>flash:</b> by default
Load the patch file on from the storage medium to the specified memory patch area	<b>patch load slot</b> <i>slot-number</i>	Required



To do...	Use the command...	Remarks
Activate the specified patches	<b>patch active</b> <i>patch-number</i> <b>slot</b> <i>slot-number</i>	<p>Required</p> <ul style="list-style-type: none"> <li>After you activate a patch, the patch takes effect and is in the test-run stage. After the switch is reset or rebooted, the patch becomes invalid.</li> <li>If you find that an ACTIVE patch is of some problem, reboot the switch to deactivate the patch, so as to avoid a series of running faults resulting from patch error.</li> </ul>
Confirm the running of the specified patches	<b>patch run</b> <i>patch-number</i> [ <b>slot</b> <i>slot-number</i> ]	<p>Required</p> <p>After you confirm the running of a patch, the patch state becomes RUNNING, and the patch is in the normal running stage. After the switch is reset or rebooted, the patch is still valid.</p>

**NOTE:**

- Set the file transfer mode to binary mode before using FTP or TFTP to upload/download patch files to/from the Flash of the switch. Otherwise, patch file cannot be parsed properly.
- This operation is applicable to patches in the ACTIVE state only.

## Step-by-step patch uninstallation

Follow these steps to stop running patches:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Stop running the specified patches	<b>patch deactivate</b> <i>patch-number</i> <b>slot</b> <i>slot-number</i>	<p>Required</p> <p>When you stop running a patch, the patch state becomes DEACTIVE, and the system runs in the way before it is installed with the patch.</p>
Delete the specified patches from the memory patch area	<b>patch delete</b> <i>patch-number</i> <b>slot</b> <i>slot-number</i>	<p>Required</p> <p>Deleting patches only removes the patches from the memory patch area, and does not delete them from the storage medium. The patches turn to the IDLE state after this operation. After a patch is deleted, the system runs in the way it did before the patch was installed.</p>

# Displaying and maintaining the software upgrade

To do...	Use the command...	Remarks
Display information about system software	<b>display boot-loader</b> [ slot <i>slot-number</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display the patch information	<b>display patch information</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view

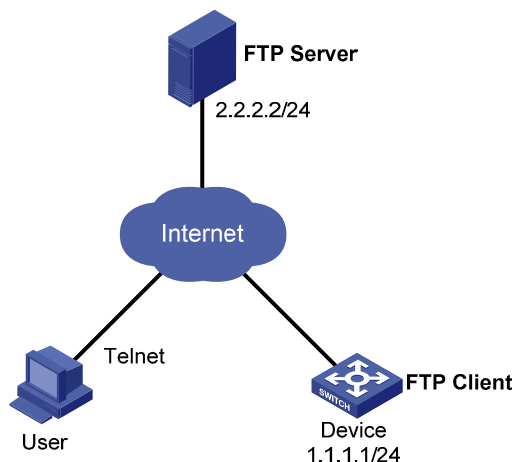
## Software upgrade configuration examples

### Scheduled upgrade configuration example

#### Network requirement

- As shown in Figure 47, the current software version is **soft-version1** for Device. Upgrade the software version of Device to **soft-version2** and configuration file to **new-config** at a time when few services are processed (for example, at 3 am) through remote operations.
- The latest application **soft-version2.bin** and the latest configuration file **new-config.cfg** are both saved in the **aaa** directory of the FTP server.
- The IP address of Device is 1.1.1.1/24, the IP address of the FTP server is 2.2.2.2/24, and Device and FTP server can reach each other.
- A user can log in to Device via Telnet, and the user and Device can reach each other.

Figure 47 Network diagram for scheduled upgrade



#### Configuration procedure

1. Configure the FTP server (configurations may vary with different types of servers)
- Set the access parameters for the FTP client (including enabling the FTP server function, setting the FTP username to **aaa** and password to **hello**, and setting the user to have access to the **flash:/aaa** directory).

```
<FTP-Server> system-view
[FTP-Server] ftp server enable
```

```
[FTP-Server] local-user aaa
[FTP-Server-luser-aaa] password cipher hello
[FTP-Server-luser-aaa] service-type ftp
[FTP-Server-luser-aaa] authorization-attribute work-directory flash:/aaa
```

- Use text editor on the FTP server to edit batch file **auto-update.txt**. The following is the content of the batch file:

```
return
startup saved-configuration new-config.cfg
boot-loader file soft-version2.bin slot 1 main
reboot
```

## 2. Configure Device

# Log in to the FTP server (The prompt may vary with servers.)

```
<Device> ftp 2.2.2.2
Trying 2.2.2.2 ...
Press CTRL+K to abort
Connected to 2.2.2.2.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(2.2.2.2:(none)):aaa
331 Give me your password, please
Password:
230 Logged in successfully
[ftp]
```

# Download file **auto-update.txt** on the FTP server.

```
[ftp] ascii
[ftp] get auto-update.txt
```

# Download file **new-config.cfg** on the FTP server.

```
[ftp]get new-config.cfg
```

# Download file **soft-version2.bin** on the FTP server.

```
[ftp] binary
[ftp] get soft-version2.bin
[ftp] bye
<Device>
```

# Change the extension of file **auto-update.txt** to **.bat**.

```
<Device> rename auto-update.txt auto-update.bat
```

To ensure correctness of the file, use the **more** command to view the content of the file.

# Execute the scheduled automatic execution function to enable Device to be automatically upgraded at 3 am.

```
<Device> system-view
[Device] job autoupdate
[Device-job-autoupdate] view system-view
[Device-job-autoupdate] time 1 one-off at 03:00 command execute auto-update.bat
```

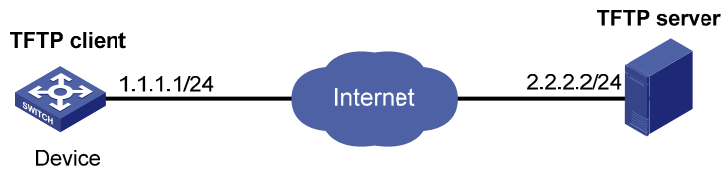
To check if the upgrade is successful after Device reboots, use the **display version** command.

# Hotfix configuration example

## Network requirements

- As shown in Figure 48, the software running on Device is having problems, and a hotfix is needed.
- The patch file **patch\_311.bin** is saved on the TFTP server.
- The IP address of Device is 1.1.1.1/24, and IP address of TFTP Server is 2.2.2.2/24. Device and TFTP server can reach each other.

Figure 48 Network diagram of hotfix configuration



## Configuration procedure

1. Configure TFTP Server. The configuration varies depending on server type and the configuration procedure is omitted.
  - Enable the TFTP server function.
  - Save the patch file **patch\_311.bin** to the directory of the TFTP server.
2. Configure Device.



### CAUTION:

Make sure the free Flash space of Device is large enough to store the patch file.

---

# Before upgrading the software, use the **save** command to save the current system configuration. The configuration procedure is omitted.

# Load the patch file **patch\_311.bin** from the TFTP server to the root directory of Device storage media.

```
<Device> tftp 2.2.2.2 get patch_311.bin
```

# Install the patch.

```
<Device> system-view
```

```
[Device] patch install flash:
```

```
Patches will be installed. Continue? [Y/N]:y
```

```
Do you want to continue running patches after reboot? [Y/N]:y
```

```
Installing patches.....
```

```
Installation completed, and patches will continue to run after reboot.
```

# Device management

Device management includes monitoring the operating status of devices and configuring their running parameters.

## NOTE:

The configuration tasks in this document are order independent. You can perform these tasks in any order.

## Configuring the device name

A device name identifies a device in a network and works as the user view prompt at the CLI. For example, if the device name is **Sysname**, the user view prompt is <Sysname>.

Follow these steps to configure the device name:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Configure the device name	<b>sysname</b> <i>sysname</i>	Optional The default device name is <b>HP</b> .

## Changing the system time

You must synchronize your device with a trusted time source by using NTP or changing the system time before you run it on the network. Network management depends on an accurate system time setting, because the timestamps of system messages and logs use the system time.

In a small-sized network, you can manually set the system time of each device.

## Configuration guidelines

You can change the system time by configuring the relative time, time zone, and daylight saving time. The configuration result depends on their configuration order (see [Table 11](#)). In the first column of this table, 1 represents the **clock datetime** command, 2 represents the **clock timezone** command, and 3 represents the **clock summer-time** command. To verify the system time setting, use the **display clock** command. This table assumes that the original system time is 2005/1/1 1:00:00.

**Table 11 System time configuration results**

Command	Effective system time	Configuration example	System time
1	<i>date-time</i>	<code>clock datetime 1:00 2007/1/1</code>	01:00:00 UTC Mon 01/01/2007
2	Original system time ± <i>zone-offset</i>	<code>clock            timezone zone-time add 1</code>	02:00:00 zone-time Sat 01/01/2005

Command	Effective system time	Configuration example	System time
1, 2	<i>date-time ± zone-offset</i>	<pre>clock datetime 2:00 2007/2/2 clock timezone zone-time add 1</pre>	03:00:00 zone-time Fri 02/02/2007
2, 1	<i>date-time</i>	<pre>clock timezone zone-time add 1 clock datetime 3:00 2007/3/3</pre>	03:00:00 zone-time Sat 03/03/2007
	The original system time outside the daylight saving time range:	<pre>clock summer-time ss one-off 1:00 2006/1/1 1:00 2006/8/8 2</pre>	01:00:00 UTC Sat 01/01/2005
3	The system time does not change until it falls into the daylight saving time range.		03:00:00 ss Sat 01/01/2005 <b>NOTE:</b>
	The original system time in the daylight saving time range:	<pre>clock summer-time ss one-off 00:30 2005/1/1 1:00 2005/8/8 2</pre>	If the original system time plus <i>summer-offset</i> is beyond the daylight saving time range, the original system time does not change. After you disable the daylight saving setting, the system time automatically decreases by <i>summer-offset</i> .
	The system time increases by <i>summer-offset</i> .		
	<i>date-time</i> outside the daylight saving time range:	<pre>clock datetime 1:00 2007/1/1 clock summer-time ss one-off 1:00 2006/1/1 1:00 2006/8/8 2</pre>	01:00:00 UTC Mon 01/01/2007
	<i>date-time</i>		10:00:00 ss Mon 01/01/2007 <b>NOTE:</b>
1, 3	<i>date-time</i> in the daylight saving time range:	<pre>clock datetime 8:00 2007/1/1 clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2</pre>	If the <i>date-time</i> plus <i>summer-offset</i> is outside the daylight saving time range, the system time equals <i>date-time</i> . After you disable the daylight saving setting, the system time automatically decreases by <i>summer-offset</i> .
	<i>date-time + summer-offset</i>		
3, 1	( <i>date-time</i> outside the daylight saving time range)	<pre>clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 clock datetime 1:00 2008/1/1</pre>	01:00:00 UTC Tue 01/01/2008

Command	Effective system time	Configuration example	System time
3, 1 ( <i>date-time</i> in the daylight saving time range)	<i>date-time</i> – <i>summer-offset</i> outside the daylight saving time range:	clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2	23:30:00 UTC Sun 12/31/2006
	<i>date-time</i> – <i>summer-offset</i>	clock datetime 1:30 2007/1/1	
	<i>date-time</i> – <i>summer-offset</i> in the daylight saving time range:	clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2	03:00:00 ss Mon 01/01/2007
	<i>date-time</i>	clock datetime 3:00 2007/1/1	
2, 3 or 3, 2	Original system clock ± <i>zone-offset</i> outside the daylight saving time range:	clock timezone zone-time add 1 clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2	02:00:00 zone-time Sat 01/01/2005
	Original system clock ± <i>zone-offset</i> + <i>summer-offset</i>	clock timezone zone-time add 1 clock summer-time ss one-off 1:00 2005/1/1 1:00 2005/8/8 2	System clock configured: 04:00:00 ss Sat 01/01/2005
1, 2, 3 or 1, 3, 2	<i>date-time</i> ± <i>zone-offset</i> outside the daylight saving time range:	clock datetime 1:00 2007/1/1 clock timezone zone-time add 1 clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2	02:00:00 zone-time Mon 01/01/2007
	<i>date-time</i> ± <i>zone-offset</i> + <i>summer-offset</i>	clock datetime 1:00 2007/1/1 clock timezone zone-time add 1 clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2	04:00:00 ss Mon 01/01/2007
2, 3, 1 or 3, 2, 1	<i>date-time</i> outside the daylight saving time range:	clock timezone zone-time add 1 clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2	01:00:00 zone-time Mon 01/01/2007
	<i>date-time</i>	clock datetime 1:00 2007/1/1	

Command	Effective system time	Configuration example	System time
	<i>date-time</i> in the daylight saving time range, but <i>date-time - summer-offset</i> outside the summer-time range:	<pre>clock      timezone zone-time add 1 clock summer-time ss one-off    1:00 2008/1/1   1:00 2008/8/8 2</pre>	23:30:00 zone-time Mon 12/31/2007
	<i>date-time - summer-offset</i>	<pre>clock datetime 1:30 2008/1/1</pre>	
	Both <i>date-time</i> and <i>date-time - summer-offset</i> in the daylight saving time range:	<pre>clock      timezone zone-time add 1 clock summer-time ss one-off    1:00 2008/1/1   1:00 2008/8/8 2</pre>	03:00:00 ss Tue 01/01/2008
	<i>date-time</i>	<pre>clock datetime 3:00 2008/1/1</pre>	

## Configuration procedure

Follow these steps to change the system time:

To do...	Use the command...	Remarks
Set the system time and date	<b>clock datetime</b> <i>time date</i>	Optional Available in user view.
Enter system view	<b>system-view</b>	—
Set the time zone	<b>clock timezone</b> <i>zone-name</i> { <b>add</b>   <b>minus</b> } <i>zone-offset</i>	Optional Universal time coordinated (UTC) time zone by default.
Set a daylight saving time scheme	Set a non-recurring scheme: <b>clock summer-time</b> <i>zone-name</i> <b>one-off</b> <i>start-time start-date</i> <i>end-time end-date add-time</i> Set a recurring scheme: <b>clock summer-time</b> <i>zone-name</i> <b>repeating</b> <i>start-time start-date</i> <i>end-time end-date add-time</i>	Optional Use either command. By default, daylight saving time is disabled, and the UTC time zone applies.

## Enabling displaying the copyright statement

The device by default displays the copyright statement when a Telnet or SSH user logs in, or when a console user quits user view. You can disable or enable the function as needed. The following is a sample copyright statement:

```
*****
* Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                *
* no decompiling or reverse-engineering shall be allowed.                  *
*****
```

Follow these steps to enable displaying the copyright statement:



To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Enable displaying the copyright statement	<b>copyright-info enable</b>	Optional Enabled by default.

# Configuring banners

## Introduction to banners

Banners are messages that the system displays when a user connects to the device to perform login authentication, and start interactive configuration.

### Banner types

You can configure the following types of banners:

- Legal banner appears after the system displays the copyright or license statement for a user attempting to log in. To continue authentication or login, the user must enter **Y** or press **Enter**. To quit the process, the user must enter **N**. **Y** and **N** are case insensitive.
- Message of the Day (MOTD) banner displays the greeting message, and appears after the legal banner and before the login banner.
- Login banner appears only when password or scheme login authentication has been configured.
- Incoming banner appears for Modem dial-in users and the shell banner appears for users that use any other access method to access the CLI.

### Message input modes

The system supports single-line input mode and multiple-line input mode for configuring a banner.

#### 1. Single-line input

In single-line input mode, all banner information comes after the command keywords in the same line. The start and end characters of the input text must be the same but are not part of the banner information. In this case, the input text, together with the command keywords, cannot exceed 510 characters.

#### 2. Multiple-line input

In multiple-line input mode, all the banner information is input in multiple lines by pressing the **Enter** key. In this case, up to 2000 characters can be input.

Multi-line input mode can be achieved in the following methods:

- Method I—Press the **Enter** key directly after the command keywords, type the banner information, and end with the % character. The **Enter** and % characters are not part of the banner information.
- Method II—Type a character after the command keywords at the first line, and then press the **Enter** key. Type the banner information, and end with the character you type at the first line. The character at the first line and the end character are not part of the banner information.
- Method III—Type multiple characters after the command keywords at the first line—with the first and last characters being different, and then press the **Enter** key. Type the banner information, and end with the first character you type at the first line. The first input character at the first line and the end character are not part of the banner information.

## Configuration procedure

Follow these steps to configure a banner:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Configure the incoming banner	<b>header incoming</b> <i>text</i>	Optional
Configure the login banner	<b>header login</b> <i>text</i>	Optional
Configure the legal banner	<b>header legal</b> <i>text</i>	Optional
Configure the shell banner	<b>header shell</b> <i>text</i>	Optional
Configure the MOTD banner	<b>header motd</b> <i>text</i>	Optional

## Banner configuration examples

# Configure the shell banner as **Welcome to HP!**.

- Single-line input mode:

```
<System> system-view
[System] header shell %Welcome to HP!%
```

- Multiple-line input mode (method I):

```
<System> system-view
[System] header shell
Please input banner content, and quit with the character '%'.
Welcome to HP!
%
```

- Multiple-line input mode (method II):

```
<System> system-view
[System] header shell W
Please input banner content, and quit with the character 'W'.
Welcome to HP!
W
```

## Configuring the exception handling method

You can configure the device to handle system exceptions in one of the following methods:

- **reboot**—The device automatically reboots to recover from the error condition.
- **maintain**—The device stays in the error condition so you can collect complete data, including error messages, for diagnosis. In this approach, you must manually reboot the device.

Follow these steps to configure the exception handling method:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Configure the exception handling method	<b>system-failure</b> { <b>maintain</b>   <b>reboot</b> }	Optional By default, the system reboots when an exception occurs.

# Rebooting the device

You can reboot the device in one of the following ways to recover from an error condition:

- Reboot the device immediately at the CLI.
- At the CLI, schedule a reboot to occur at a specific time and date or after a delay.
- Power off and then re-power on the device. This method might cause data loss and hardware damage, and is the least preferred method.

Reboot at the CLI enables easy remote device maintenance.

## ⚠ CAUTION:

- A reboot can interrupt network services.
- To avoid data loss, use the **save** command to save the current configuration before a reboot.
- Use the **display startup** and **display boot-loader** commands to check that you have correctly set the startup configuration file and the main system software image file. If the main system software image file has been corrupted or does not exist, the device cannot reboot. You must re-specify a main system software image file, or power off the device and then power it on so the system can reboot with the backup system software image file.

## Rebooting the device immediately at the CLI

Perform the following command in user view to reboot the device:

To do...	Use the command...	Remarks
Reboot the device immediately	<b>reboot</b> [ slot <i>slot-number</i> ]	Required The <i>slot-number</i> argument must be 1.

## Scheduling a device reboot

Perform one of the following commands in user view to schedule a device reboot:

To do...	Use the command...	Remarks
Schedule a reboot to occur at a specific time and date	<b>schedule reboot at</b> <i>hh:mm</i> [ <i>date</i> ]	Required Use either command.
Schedule a reboot to occur after a delay	<b>schedule reboot delay</b> { <i>hh:mm</i>   <i>mm</i> }	The scheduled reboot function is disabled by default. The two commands overwrite each other.

## NOTE:

- The system displays the alert "REBOOT IN ONE MINUTE" one minute before the reboot.
- For data security, if you are performing file operations at the reboot time, the system does not reboot.

# Scheduling jobs

You can schedule a job to automatically run a command or a set of commands without administrative interference. The commands in a job are polled every minute. When the scheduled time for a command is reached, the job automatically executes the command. If a confirmation is required while the command is running, the system automatically inputs Y or Yes. If characters are required, the system automatically inputs a default character string, or inputs an empty character string when there is no default character string.

## Job configuration approaches

You can configure jobs in a non-modular or modular approach. Use the non-modular approach for a one-time command execution and use non-modular approach for complex maintenance work.

**Table 12 A comparison of non-modular and modular approaches**

Comparison item	Scheduling a job in the non-modular approach	Scheduling a job in the modular approach
Configuration method	Configure all elements in one command	Separate job, view, and time settings
Can multiple jobs be configured?	No	Yes
Can a job have multiple commands?	No	Yes
Supported views	User view (represented by <b>shell</b> ), system view	All views ( <b>monitor</b> represents user view)
Supported commands	Commands in user view and system view	Commands in any view
Can a job be repeatedly executed?	No	Yes
Can a job be saved to the configuration file?	No	Yes

## Configuration guidelines

- To have a job successfully run a command, check that the specified view and command are valid. The system does not verify their validity.
- The configuration interface, view, and user status that you have before job execution restores even if the job has run a command that changes the user interface (for example, **telnet**, **ftp**, and **ssh2**), the view (for example, **system-view** and **quit**), or the user status (for example, **super**).
- The jobs run in the background without displaying any messages except log, trap and debugging messages.
- In the modular approach:
  - Every job can have only one view and up to 10 commands. If you specify multiple views, the one specified the last takes effect.
  - Input a view name in its complete form. Most commonly used view names include **monitor** for user view, **system** for system view, and **Vlan-interface** for VLAN interface view.
  - The time ID (*time-id*) must be unique in a job. If two time and command bindings have the same time ID, the one configured last takes effect.

## Scheduling a job in the non-modular approach

Perform one of the following commands in user view to schedule a job:

To do...	Use the command...	Remarks
Schedule a job to run a command at a specific time	<b>schedule job at</b> <i>time</i> [ <i>date</i> ] <b>view</b> <i>view command</i>	Required Use either command. <b>NOTE:</b>
Schedule a job to run a command after a delay	<b>schedule job delay</b> <i>time</i> <b>view</b> <i>view</i> <i>command</i>	If you change the system time by using the <b>clock datetime</b> , <b>clock summer-time</b> , or <b>clock timezone</b> command after you configure a scheduled job, the job configuration becomes invalid automatically.

## Scheduling a job in the modular approach

Follow these steps to configure a scheduled job:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Create a job and enter job view	<b>job</b> <i>job-name</i>	Required
Specify the view in which the commands in the job run	<b>view</b> <i>view-name</i>	Required You can specify only one view for a job. The job executes all commands in the specified view.
Add commands to the job	Configure a command to run at a specific time and date: <b>time</b> <i>time-id</i> <b>at</b> <i>time date</i> <b>command</b> <i>command</i> Configure a command to run at a specific time <b>time</b> <i>time-id</i> { <b>one-off</b>   <b>repeating</b> } <b>at</b> <i>time</i> [ <b>month-date</b> <i>month-day</i>   <b>week-day</b> <i>week-daylist</i> ] <b>command</b> <i>command</i> Configure a command to run after a delay: <b>time</b> <i>time-id</i> { <b>one-off</b>   <b>repeating</b> } <b>delay</b> <i>time</i> <b>command</b> <i>command</i>	Required Use any of the commands. <b>NOTE:</b> Changing the system time does not affect the execution time of the job set by the <b>time at</b> command or the <b>time delay</b> command.

## Disabling Boot ROM access

By default, anyone can press **Ctrl+B** during startup to enter the Boot menu and configure the Boot ROM. To protect the system, you can disable Boot ROM access so the users can access only the CLI.

You can also set a Boot ROM password the first time you access the Boot menu to protect the Boot ROM.

To view Boot ROM accessibility status, use the **display startup** command. For more information about the **display startup** command, see the *Fundamentals Command Reference*.

Follow the step below to disable Boot ROM access:

To do...	Use the command...	Remarks
Disable Boot ROM access	<b>undo startup bootrom-access enable</b>	Required By default, Boot ROM access is enabled. Available in user view.

## Configuring the detection timer

Some protocols might shut down ports under specific circumstances. For example, MSTP shuts down a BPDU guard enabled port when the port receives a BPDU. Then, the device starts the detection timer. If the port is still down when the detection timer expires, the port quits the shutdown status and resume its actual physical status.

Follow these steps to configure the detection timer:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—
Configure the detection timer	<b>shutdown-interval</b> <i>time</i>	Optional The detection interval is 30 seconds by default.

## Configuring temperature alarm thresholds (available only on the A3100 v2 EI)

You can set the temperature alarm thresholds to monitor the temperature of a device.

The temperature alarm thresholds include lower temperature limit, warning temperature threshold, and temperature alarming threshold.

When the device temperature drops below the lower limit or reaches the warning threshold, the device logs the event and outputs a log message and a trap.

When the device temperature reaches the alarming threshold, the device constantly outputs log and trap messages to the configuration terminal and lights the temperature alarm LED on the device panel.

Follow these steps to configure temperature alarm thresholds:

To do...	Use the command...	Remarks
Enter system view	<b>system-view</b>	—

To do...	Use the command...	Remarks
Configure temperature alarm thresholds	<b>temperature-limit slot</b> <i>slot-number</i> <b>inflow sensor-number lowerlimit warninglimit</b> [ <i>alarmlimit</i> ]	Optional By default : <ul style="list-style-type: none"> <li>The lower temperature limit is 5°C (41°F).</li> <li>The warning temperature threshold is 70°C (158°F).</li> <li>The Alarming temperature threshold is 80°C (176°F).</li> </ul> The warning and alarming thresholds must be higher than the lower temperature limit. The alarming threshold must be higher than the warning threshold.

**NOTE:**

This feature is available only on PoE-capable models of the A3100 v2 EI Switch Series.

## Clearing idle 16-bit interface indexes

The device must maintain persistent 16-bit interface indexes and keep one interface index match one interface name for network management. After deleting a logical interface, the device retains its 16-bit interface index so the same index can be assigned to the interface at interface re-creation.

To avoid index depletion causing interface creation failures, you can clear all 16-bit indexes that have been assigned but not in use. The operation does not affect the interface indexes of the interfaces that have been created but the indexes assigned to re-created interfaces might change.

Follow the step below to clear idle 16-bit interface indexes:

To do...	Use the command...	Remarks
Clear idle 16-bit interface indexes	<b>reset unused porttag</b>	Required Available in user view.

**NOTE:**

A confirmation is required when you execute this command. The command will not run if you fail to make a confirmation within 30 seconds or enter **N** to cancel the operation.

## Verifying and diagnosing transceiver modules

### Verifying transceiver modules

You can verify the genuineness of a transceiver module in the following ways:

- Display the key parameters of a transceiver module, including its transceiver type, connector type, central wavelength of the transmit laser, transfer distance and vendor name.

- Display its electronic label. The electronic label is a profile of the transceiver module and contains the permanent configuration including the serial number, manufacturing date, and vendor name. The data is written to the storage component during debugging or testing.

Perform the following commands in any view to verify transceiver modules:

To do...	Use the command...
Display key parameters of transceiver modules	<b>display transceiver interface</b> [ <i>interface-type</i> <i>interface-number</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]
Display transceiver modules' electronic label information	<b>display transceiver manuinfo interface</b> [ <i>interface-type</i> <i>interface-number</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]

**NOTE:**

The **display transceiver manuinfo** command cannot display information for some transceiver modules.

## Diagnosing transceiver modules

The device provides the alarm function and digital diagnosis function for transceiver modules. When a transceiver module fails or inappropriately work, you can check for alarms present on the transceiver module to identify the fault source or examine the key parameters monitored by the digital diagnosis function, including the temperature, voltage, laser bias current, TX power, and RX power.

Perform the following commands in any view to diagnose transceiver modules:

To do...	Use the command...
Display alarms present on transceiver modules	<b>display transceiver alarm interface</b> [ <i>interface-type</i> <i>interface-number</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]
Display the present measured values of the digital diagnosis parameters for pluggable transceivers	<b>display transceiver diagnosis interface</b> [ <i>interface-type</i> <i>interface-number</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]

**NOTE:**

The **display transceiver diagnosis** command cannot display information for some transceiver modules.

## Displaying and maintaining device management configuration

For diagnosis or troubleshooting, you can use separate **display** commands to collect running status data module by module, or use the **display diagnostic-information** command to bulk collect running data for multiple modules. The **display diagnostic-information** command equals this set of commands: **display clock**, **display version**, **display device**, and **display current-configuration**.

To do...	Use the command...	Remarks
Display system version information	<b>display version</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view



To do...	Use the command...	Remarks
Display the system time and date	<b>display clock</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display or save operating statistics for multiple feature modules	<b>display diagnostic-information</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display CPU usage statistics	<b>display cpu-usage</b> [ <i>slot slot-number</i> [ <i>cpu cpu-number</i> ] ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ] <b>display cpu-usage</b> <i>entry-number</i> [ <i>offset</i> ] [ <b>verbose</b> ] [ <i>slot slot-number</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display historical CPU usage statistics in charts	<b>display cpu-usage history</b> [ <i>task task-id</i> ] [ <i>slot slot-number</i> [ <i>cpu cpu-number</i> ] ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display hardware information	<b>display device</b> [ [ <i>slot slot-number</i> [ <i>subslot subslot-number</i> ] ]   <b>verbose</b> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display the electronic label data for the device	<b>display device manuinfo</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display device temperature statistics	<b>display environment</b> [ <i>slot slot-number</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view This command is available on only PoE-capable models of the A3100 v2 EI Switch Series.
Display the operating state of fans	<b>display fan</b> [ <i>fan-id</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view This command is available on only PoE-capable models of the A3100 v2 EI Switch Series.
Display memory usage statistics	<b>display memory</b> [ <i>slot slot-number</i> [ <i>cpu cpu-number</i> ] ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display the power state	<b>display power</b> [ <i>power-id</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display RPS state information	<b>display rps</b> [ <i>rps-id</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view This feature is available on only A3100-24-PoE v2 EI Switch(JD313B) and A3100-16-PoE v2 EI Switch(JD312B) models.
Display the mode of the last reboot	<b>display reboot-type</b> [ <i>slot slot-number</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display the configuration of the job configured by using the <b>schedule job</b> command	<b>display schedule job</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view

To do...	Use the command...	Remarks
Display the device reboot setting	<b>display schedule reboot</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display the configuration of jobs configured by using the <b>job</b> command	<b>display job</b> [ <i>job-name</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display the exception handling method	<b>display system-failure</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display the device software version update history	<b>display version-update-record</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Clear the device software version update history	<b>reset version-update-record</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in system view

---

# Automatic configuration

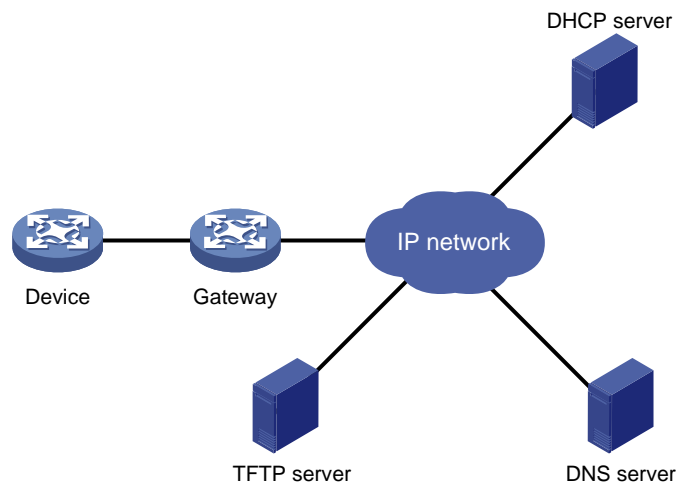
## Automatic configuration overview

Automatic configuration enables a device without any configuration file to automatically obtain and execute a configuration file during startup. Automatic configuration simplifies network configuration, facilitates centralized management, and reduces maintenance workload.

To implement automatic configuration, the network administrator saves configuration files on a server and a device automatically obtains and executes a specific configuration file.

## Typical automatic configuration network

Figure 49 Network diagram for automatic configuration



As shown in Figure 49, the device implements automatic configuration with the cooperation of the following servers: a DHCP server, TFTP server, and DNS server:

- DHCP server—assigns an IP address and other configuration parameters such as the configuration file name, TFTP server IP address, and DNS server IP address to the device.
- TFTP server: Saves files needed in automatic configuration such as the host name file and the configuration file.
- DNS server—resolves between IP addresses and host names. In some cases, the device resolves its IP address to the host name through the DNS server, and then uses the host name to request the configuration file with the same name (**hostname.cfg**) from the TFTP server. If the device gets the domain name of the TFTP server from the DHCP response, the device can also resolve the domain name of the TFTP server to the IP address of the TFTP server through the DNS server.

If the DHCP server, TFTP server, DNS server, and the device are not in the same network segment, you need to configure the DHCP relay agent on the gateway.

# How automatic configuration works

Automatic configuration works in the following manner:

1. During startup, the device sets the first up interface (if up Layer 2 Ethernet interfaces are available, the VLAN interface of the default VLAN of the Ethernet interfaces is selected as the first up interface.) as the DHCP client to request parameters from the DHCP server, such as an IP address and name of a TFTP server, IP address of a DNS server, and the configuration file name.
2. After getting related parameters, the device sends a TFTP request to obtain the configuration file from the specified TFTP server and executes the configuration file. If the client cannot get such parameters, it uses factory default configuration.

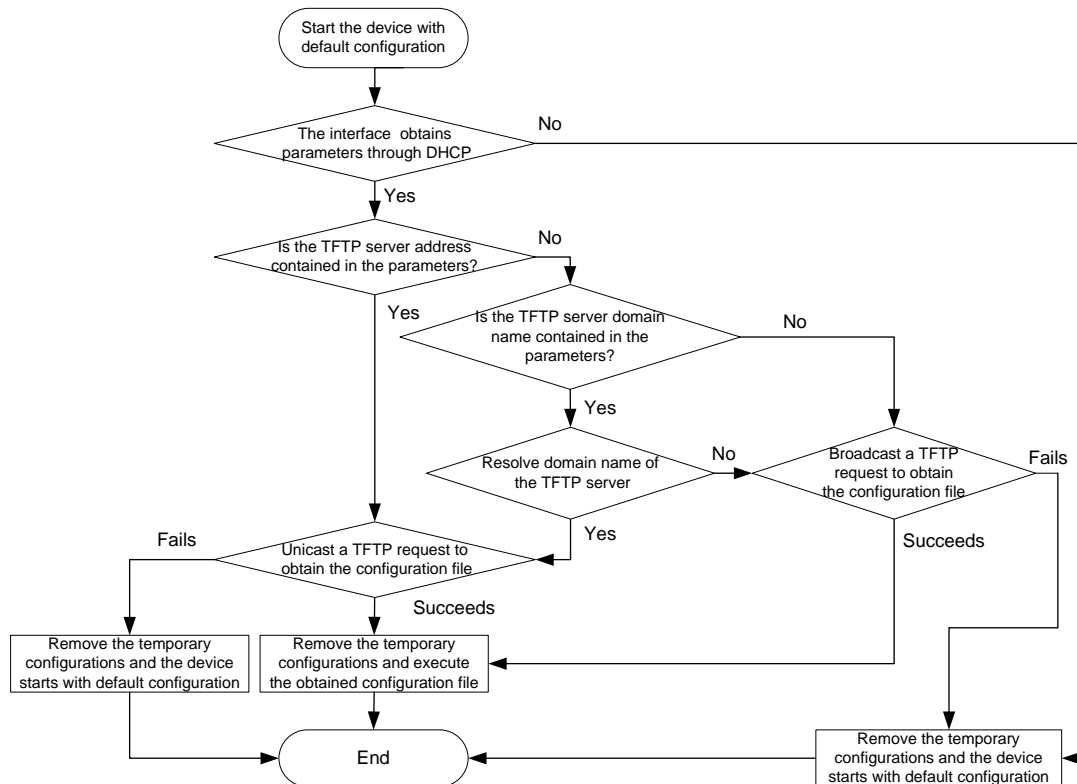
**NOTE:**

- To implement automatic configuration, you need to configure the DHCP server, DNS server and TFTP server, but you do not need to perform any configuration on the device that performs automatic configuration.
- Before starting the device, connect only the interface needed in automatic configuration to the network.

## Work flow of automatic configuration

Figure 50 shows the work flow of automatic configuration.

**Figure 50 Work flow of automatic configuration**



# Using DHCP to obtain an IP address and other configuration information

## Address acquisition process

As mentioned before, a device sets the first up interface as the DHCP client during startup. The DHCP client broadcasts a DHCP request, where the Option 55 field specifies the information that the client wants to obtain from the DHCP server such as the configuration file name, domain name and IP address of the TFTP server, and DNS server IP address.

After receiving the DHCP response from the DHCP server, the device obtains the IP address and resolves the following fields in the DHCP response:

- Option 67 or the file field that specifies the configuration file name. If Option 67 contains the configuration file name, the device does not resolve the file field. If not, the device resolves the file field.
- Option 66 that specifies the TFTP server domain name
- Option 150 that specifies the TFTP server IP address
- Option 6 that specifies the DNS server IP address.

If no response is received from the DHCP server, the device removes the temporary configuration and starts up with factory defaults.

---

### NOTE:

- The configuration file name is saved in the Option 67 or file field of the DHCP response. The device first resolves the Option 67 field. If this field contains the configuration file name, the device does not resolve the file field. If not, it resolves the file field.
  - The temporary configuration contains two parts: the configuration made on the interface through which automatic configuration is performed, and the configuration made by executing the **ip host** commands in the host name file (For more information about the **ip host** command, see the *Layer 3—IP Services Command Reference*). The temporary configuration is removed by executing the **undo** commands.
  - For more information about DHCP, see the *Layer 3—IP Services Configuration Guide*.
- 

## Principles for selecting an address pool on the DHCP server

The DHCP server selects IP addresses and other network configuration parameters from an address pool for clients. DHCP supports the following types of address pools:

- Dynamic address pool: A dynamic address pool contains a range of IP addresses and other parameters that the DHCP server dynamically assigns to clients.
- Static address pool: A static address pool contains the binding of an IP address and a MAC address (or a client ID). The DHCP server assigns the IP address of the binding and specific configuration parameters to a requesting client whose MAC address or ID is contained in the binding. In this way, the client can get a fixed IP address.

Select address pools by using one of the following methods.

- If devices use the same configuration file, you can configure a dynamic address pool on the DHCP server to assign IP addresses and the same configuration parameters (for example, configuration file name) to the devices. The configuration file can only contain common configurations of the devices, and the specific configurations of each device need to be performed in other ways. For example, the configuration file can enable Telnet and create a local user on devices so that the

administrator can Telnet to each device to perform specific configurations (for example, configure the IP address of each interface).

- If devices use different configuration files, you need to configure static address pools to ensure that each device can get a fixed IP address and a specific configuration file. With this method, the administrator does not need to perform any other configuration for the devices.

---

**NOTE:**

To configure static address pools, you must obtain client IDs. To obtain a device's client ID, use the **display dhcp server ip-in-use** command to display address binding information on the DHCP server after the device obtains its IP address through DHCP.

---

## Obtaining the configuration file from the TFTP server

### File types

A device can obtain the following files from the TFTP server during automatic configuration:

- The configuration file specified by the Option 67 or file field in the DHCP response
- The host name file named **network.cfg**, which stores mappings between IP addresses and host names.

For example, the host name file can include the following:

```
ip host host1 101.101.101.101
ip host host2 101.101.101.102
ip host client1 101.101.101.103
ip host client2 101.101.101.104
```

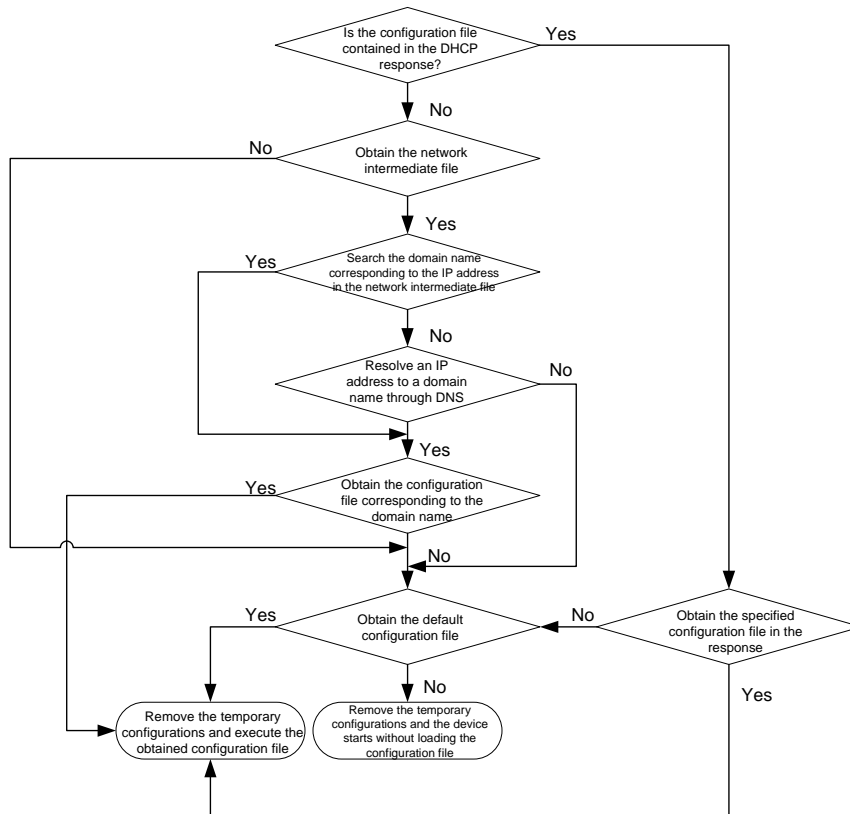
---

**△ CAUTION:**

- There must be a space before the keyword **ip host**.
  - The host name of a device saved in the host name file must be the same as the configuration file name of the device, and can be identical with or different from that saved in the DNS server.
- 
- The configuration file of a device is named **hostname.cfg**, where **hostname** is the host name of the device. For example, if the host name of a device is **aaa**, the configuration file of the device is named **aaa.cfg**.
  - The default configuration file is named **device.cfg**.

## Obtaining the configuration file

Figure 51 Obtain the configuration file



A device obtains its configuration file by using the following workflow:

- If the DHCP response contains the configuration file name, the device requests the specified configuration file from the TFTP server.
- If not, the device tries to get its host name from the host name file obtained from the TFTP server. If it fails, the device resolves its IP address to the host name through DNS server. Once the device gets its host name, it requests the configuration file with the same name from the TFTP server.
- If all the operations fail, the device requests the default configuration file from the TFTP server.

## TFTP request sending mode

The device selects to unicast or broadcast a TFTP request by using the following workflow:

- If a legitimate TFTP server IP address is contained in the DHCP response, the device unicasts a TFTP request to the TFTP server.
- If not, the device resolves the TFTP server domain name contained in the DHCP response to the IP address through the DNS server. If successful, the device unicasts a TFTP request to the TFTP server; if not, the device broadcasts a TFTP request.
- If the IP address and the domain name of the TFTP server are not contained in the DHCP response or they are illegitimate, the device broadcasts a TFTP request.

---

**NOTE:**

After broadcasting a TFTP request, the device selects the TFTP server that responds first to obtain the configuration file. If the requested configuration file does not exist on the TFTP server, the request operation fails, and the device removes the temporary configuration and starts up with factory defaults.

---

## Executing the configuration file

After obtaining the configuration file, the device removes the temporary configuration and executes the configuration file. If no configuration file is obtained, the device removes the temporary configuration and starts up with factory defaults.

---

**NOTE:**

The configuration file is deleted after executed. Save the configuration by using the **save** command. Otherwise, the device has to perform automatic configuration again after reboot. For more information about the **save** command, see the *Fundamentals Command Reference*.

---



---

# Support and other resources

## Contacting HP

For worldwide technical support information, see the HP support website:

<http://www.hp.com/support>

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

## Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

<http://www.hp.com/go/wwalerts>

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

## Related information

### Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

<http://www.hp.com/support/manuals>

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP A-Series Acronyms*.

### Websites

- HP.com <http://www.hp.com>
- HP Networking <http://www.hp.com/go/networking>
- HP manuals <http://www.hp.com/support/manuals>
- HP download drivers and software <http://www.hp.com/support/downloads>
- HP software depot <http://www.software.hp.com>
- HP Education <http://www.hp.com/learn>

# Conventions

This section describes the conventions used in this documentation set.





## Command conventions

Convention	Description
<b>Boldface</b>	<b>Bold</b> text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	<i>Italic</i> text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x   y   ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[ x   y   ... ]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x   y   ... } *	Asterisk-marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[ x   y   ... ] *	Asterisk-marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

## GUI conventions

Convention	Description
<b>Boldface</b>	Window names, button names, field names, and menu items are in bold text. For example, the <b>New User</b> window appears; click <b>OK</b> .
>	Multi-level menus are separated by angle brackets. For example, <b>File &gt; Create &gt; Folder</b> .

## Symbols

Convention	Description
 <b>WARNING</b>	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 <b>CAUTION</b>	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
 <b>IMPORTANT</b>	An alert that calls attention to essential information.
<b>NOTE</b>	An alert that contains additional or supplementary information.
 <b>TIP</b>	An alert that provides helpful information.

## Network topology icons

	Represents a generic network device, such as a router, switch, or firewall.
---	---



Represents a generic network device, such as a router, switch, or firewall.

---



Represents a routing-capable device, such as a router or Layer 3 switch.

---



Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.

---

## Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

---

# Index

## [A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [H](#) [L](#) [M](#) [N](#) [O](#) [P](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#)

### A

Automatic configuration overview, [140](#)

### B

Backing up the startup configuration file, [112](#)

### C

Changing the system time, [126](#)

Checking command-line errors, [8](#)

Clearing idle 16-bit interface indexes, [136](#)

CLI view description, [2](#)

Command conventions, [1](#)

Configuration file overview, [106](#)

Configuring banners, [130](#)

Configuring HTTP login, [66](#)

Configuring HTTPS login, [67](#)

Configuring login control over Telnet users, [78](#)

Configuring NMS login, [74](#)

Configuring source IP-based login control over NMS users, [81](#)

Configuring source IP-based login control over web users, [83](#)

Configuring temperature alarm thresholds (available only on the A3100 v2 EI), [135](#)

Configuring the detection timer, [135](#)

Configuring the device name, [126](#)

Configuring the exception handling method, [131](#)

Configuring the FTP client, [86](#)

Configuring the FTP server, [91](#)

Configuring the TFTP client, [97](#)

Configuring user privilege and command levels, [13](#)

Contacting HP, [146](#)

Controlling the CLI display, [10](#)

Conventions, [147](#)

### D

Deleting a startup configuration file, [112](#)

Disabling Boot ROM access, [134](#)

Displaying and maintaining a configuration file, [113](#)

Displaying and maintaining CLI, [20](#)

Displaying and maintaining CLI login, [64](#)

Displaying and maintaining device management configuration, [137](#)

Displaying and maintaining FTP, [95](#)

Displaying and maintaining the software upgrade, [123](#)

Displaying and maintaining the TFTP client, [98](#)

Displaying and maintaining web login, [70](#)

### E

Enabling displaying the copyright statement, [129](#)

Entering the CLI, [1](#)

Example for file operations, [104](#)

### F

FTP overview, [85](#)

### H

How automatic configuration works, [141](#)

### L

Logging in through modems, [52](#)

Logging in through SSH, [47](#)

Logging in through Telnet, [36](#)

Logging in through the console port, [24](#)

Login methods, [21](#)

### M

Managing files, [100](#)

### N

NMS login example, [75](#)

NMS login overview, [74](#)

### O

Overview, [24](#)

### P

Performing batch operations, [103](#)

Performing directory operations, [100](#)

Performing file operations, [101](#)

Performing storage medium operations, [104](#)

### R

Rebooting the device, [132](#)

Related information, [146](#)

Restoring a startup configuration file, [113](#)

## S

Saving the current configuration, [20](#)

Saving the running configuration, [107](#)

Scheduling jobs, [133](#)

Setting configuration rollback, [108](#)

Setting prompt modes, [104](#)

Software upgrade by installing hotfixes, [117](#)

Software upgrade configuration examples, [123](#)

Software upgrade methods, [115](#)

Specifying a startup configuration file to be used at the next system startup, [111](#)

Switch software overview, [115](#)

## T

TFTP client configuration example, [98](#)

TFTP overview, [96](#)

Typical automatic configuration network, [140](#)

Typing commands, [5](#)

## U

Undo form of a command, [2](#)

Upgrading system software through a system reboot, [117](#)

Upgrading the Boot ROM program through a system reboot, [116](#)

User interface overview, [22](#)

User login control methods, [78](#)

Using command history, [8](#)

Using the CLI online help, [4](#)

## V

Verifying and diagnosing transceiver modules, [136](#)

## W

Web login example, [70](#)

Web login overview, [66](#)

What is CLI?, [1](#)